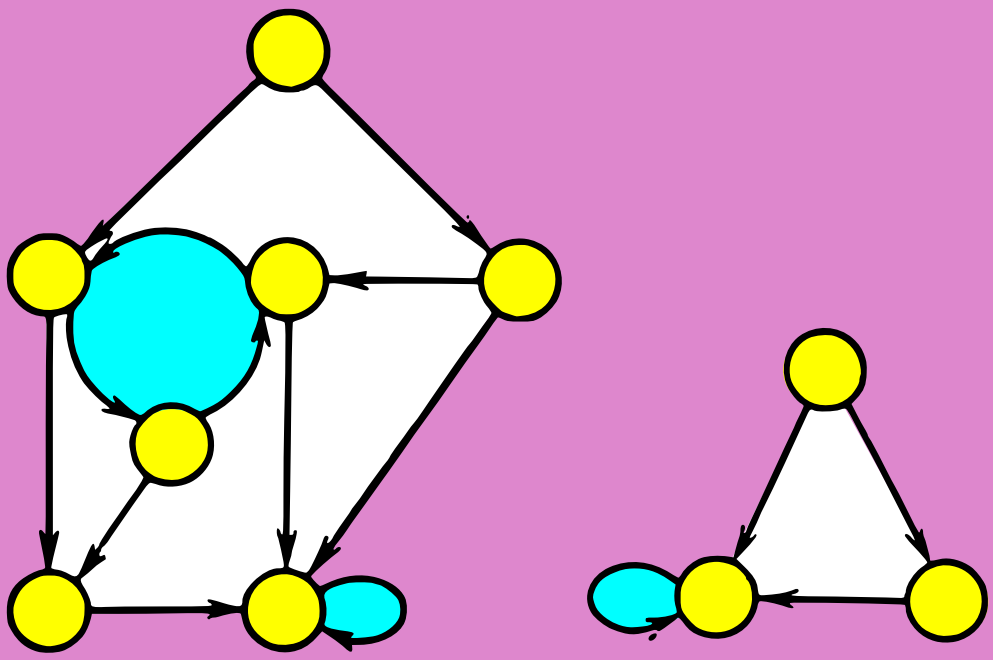
M. Kargapolov, I. Merzliakov

ÉLÉMENTS DE LA THÉORIE DES GROUPES



Éditions Mir Moscou

М. И. КАРГАПОЛОВ
Ю. И. МЕРЗЛЯКОВ

ОСНОВЫ ТЕОРИИ ГРУПП

ИЗДАТЕЛЬСТВО «НАУКА»
МОСКВА

M. KARGAPOLOV, Iou. MERZLIAKOV

ÉLÉMENTS DE LA THÉORIE DES GROUPES

ÉDITIONS MIR • MOSCOU

Traduit du russe
par V. KOTLIAR

На французском языке

© Издательство «Наука». Главная редакция физико-математической литературы, 1982, с изменениями

© Traduction française Editions Mir 1985

PRÉFACE À L'ÉDITION FRANÇAISE

Ce livre réunit les notes des conférences sur la théorie des groupes lues par les auteurs en 1968-1970 à l'Université de Novossibirsk. On y expose précisément les éléments, sans entrer dans le détail ni s'enliser dans les généralisations. Nous espérons que ces notes serviront de point de départ au lecteur intéressé par la théorie des groupes et lui permettront de passer rapidement à des ouvrages plus spéciaux dans cette discipline.

Nous nous gardions soigneusement de franchir le pas entre la théorie abstraite et la théorie scholastique, en expliquant dans la mesure du possible les notions compliquées par des exemples faciles. Les exemples accompagnant le texte sont de quatre types : les nombres pour l'addition, les nombres pour la multiplication, les permutations, les matrices. Pour comprendre le texte proprement dit, le cours d'algèbre générale suffit ; par contre, les exemples demandent parfois des connaissances un peu plus approfondies. Les exemples et les exercices étant d'utiles compléments au texte, nous déconseillons vivement au lecteur de les sauter en première lecture et de remettre leur solution à plus tard.

De temps en temps nous signalons des questions non encore résolues. Le lecteur trouvera une liste assez complète des questions ouvertes de la théorie des groupes, qui reflètent les intérêts d'un large cercle de spécialistes, dans l'édition la plus récente du Cahier de Kourovka [36].

En plus des trois éditions en langue russe (Moscou, 1972, 1977, 1982), le présent ouvrage a été traduit en polonais (Varsovie, 1976) et en anglais (New York, 1979). C'est d'après la 3-ième édition russe, la plus complète (le chapitre 8 a été ajouté), que cette traduction française est établie.

Le destin est impitoyable, et voilà que je me trouve seul à signer cette préface : le 20 février 1976 Mikhaïl Ivanovitch Kargapolov décédait dans sa 48-ième année, à la suite d'une longue et grave maladie. Puisse le théorème 25.2.1, « le plus profond des théorèmes sur les groupes résolubles » [31] figurant désormais dans ce livre, être un hommage à ce mathématicien remarquable et homme cordial.

Iou. Merzliakov

Novossibirsk, Academgorodok
Le 25 janvier 1984

NOTATIONS CANONIQUES

Afin de faciliter la lecture, nous citons les notations « personnalisées » des êtres classiques, respectées partout dans le livre, et les pages où ces notations sont introduites et expliquées:

$\mathbf{A}_n$	20
$\mathbf{A}_{\mathfrak{n}}$	105
$\mathbf{B}_r(m)$	191
$\mathbf{C}$	17
$\mathbf{C}^*$	17
$\mathbb{C}_n$	17
$\mathbf{C}_{p^\infty}$	17
$\mathbf{D}_n(K)$, $\mathbf{D}_n(K, \alpha)$	18, 44
$\mathbf{F}(X)$	110
$\mathbf{F}_n(X)$, $\mathbf{F}_n$	111
$\mathbf{F}_\infty(X)$, $\mathbf{F}_\infty$	111
$\mathbf{F}_V(X)$, $\mathbf{F}_{\mathfrak{n}}(\mathfrak{L})$	124
$\mathbf{GF}(q)$	17
$\mathbf{GF}(q)^*$	17
$\mathbf{GL}_n(K)$, $\mathbf{GL}_n(K, \alpha)$	17, 44
$\mathbf{M}_n(K)$	18
$\mathbf{O}_n(K)$, $\mathbf{O}_n(K, \alpha)$	21, 44
$\mathbf{PSL}_n(K)$	105
$\mathbb{Q}$	17
$\mathbb{Q}^*$	17
$\mathbb{Q}_p$	17
$\mathbb{Q}_{p^\infty}$	55
$\mathbb{R}$	17
$\mathbb{R}^*$	17
$\mathbf{S}(M)$	17
$\mathbf{S}_n$	17
$\mathbf{S}_{\mu}(M)$	105
$\mathbf{SL}_n(K)$, $\mathbf{SL}_n(K, \alpha)$	18, 44
$\mathbf{T}_n(K)$, $\mathbf{T}_n(K, \alpha)$	18, 44
$\mathbf{U}_n$	21

$\mathbf{UT}_n(K)$, $\mathbf{UT}_n(K, \mathfrak{a})$	18, 44
$\mathbf{UT}_n^m(K)$, $\mathbf{UT}_n^m(K, \mathfrak{a})$	21, 44
$\mathbb{Z}$	17
$\mathbb{Z}^*$	17
$\mathbb{Z}_n$	17
$\mathbb{Z}_n^*$	17
$\mathbb{Z}_{p^\infty}$	54
$\Gamma_n(m)$, $\Gamma_n(\mathfrak{a})$	44, 130

INTRODUCTION

Pourquoi un carré nous semble-t-il symétrique, un cercle encore plus symétrique, et le chiffre 4 pas symétrique du tout? Pour répondre à cette question, considérons les déplacements après lesquels la figure reste elle-même. On comprend sans peine qu'il y a huit opérations de ce type pour le carré, une infinité pour le cercle, et une seule pour le chiffre 4 : c'est le déplacement identique qui laisse chaque point de la figure à sa place. En considérant l'ensemble G de tous les déplacements qui envoient la figure sur elle-même, on peut dire si elle est symétrique ou non : plus G est vaste, et plus la symétrie est grande. Introduisons une loi de composition sur G, c'est-à-dire une opération définie sur les éléments de G, en disant que si x, y sont deux déplacements appartenant à G, leur composé (ou produit) est un troisième déplacement qu'on obtient en faisant d'abord x et ensuite y. Par exemple, x et y sont les symétries du carré par rapport à ses diagonales : alors $x \cdot y$ est la rotation de 180° autour du centre du carré.

De toute évidence, la loi de composition introduite sur G possède les propriétés suivantes : 1° $(xy)\,z = x\,(yz)$ pour x, y, z quelconques de G ; 2° il existe dans G un élément e tel que $xe = ex = x$ pour tout x de G ; 3° pour tout x de G il existe dans G un x^{-1} tel que $xx^{-1} = x^{-1}x = e$. En effet, on peut prendre pour e le déplacement identique et pour x^{-1} le déplacement inverse de x, c'est-à-dire celui qui ramène chaque point déplacé par x à sa place initiale.

De cet exemple, passons à un ensemble arbitraire G muni d'une loi de composition, i.e. tel que pour ses deux éléments quelconques x, y il existe dans G un troisième élément xy. Si les conditions 1°, 2°, 3° sont vérifiées comme précédemment, on dit que l'ensemble G muni de la loi de composition indiquée est un *groupe*.

Les groupes sont un des principaux types de structures algébriques, et la théorie des groupes, un des chapitres de base de l'algèbre contemporaine. Il a fallu plusieurs générations de mathématiciens, plus de cent ans au total, pour que le concept de groupe devienne aussi limpide qu'aujourd'hui. De Lagrange qui se sert intuitivement

des groupes de permutations pour résoudre des équations algébriques par radicaux (1771), en passant par les recherches de Ruffini (1799) et d'Abel (1824), jusqu'à Evariste Galois qui utilise déjà à bon escient l'idée d'un groupe (et qui introduit d'ailleurs le terme), tel est le chemin suivi par cette idée dans la filière de la théorie des équations algébriques. D'une façon indépendante et pour d'autres raisons, elle apparaît au milieu du XIXe siècle en géométrie, au moment où *la* Géométrie antique cède la place à *des* géométries multiples et variées, posant la question d'affinité entre elles. La solution est proposée dans le *Programme d'Erlangen* de Klein (1872) où la classification des groupes est fondée sur la notion d'un groupe de transformations. La troisième source de la notion de groupe est la théorie des nombres. Citons ici le travail d'Euler sur les résidus de la division des puissances (1761) et le travail de Gauss sur la composition des formes quadratiques binaires (1801).

A la fin du XIXe siècle, ayant compris que les différentes idées sur les groupes reposent sur un concept unique malgré la diversité des champs d'application, des mathématiciens tels que Cayley, Frobenius, von Dyck ont créé la notion moderne de groupe abstrait. C'était un des premiers exemples de structure algébrique abstraite. Il aura servi de modèle à bien des égards pendant les rénovations survenues au début du XXe siècle tant en algèbre que dans l'édifice mathématique en général: ce changement allait être, de ce fait, moins dramatique. L'étude des groupes, libérée de l'impératif de finitude et indifférente à la nature des éléments, devient une discipline mathématique à part entière avec la parution de la *Théorie abstraite des groupes* de O. Iou. Schmidt (1916).

A l'heure actuelle, la théorie des groupes est un des domaines les plus évolués de l'algèbre. Elle a de multiples applications tant en mathématiques qu'au-delà de leurs frontières: en topologie, théorie des fonctions, cristallographie, mécanique quantique et dans bien d'autres domaines des mathématiques et des sciences naturelles. Le but final de la théorie des groupes en tant que telle est de décrire toutes les compositions ayant une structure de groupe.

Citons quelques exemples d'application des groupes en algèbre, en mathématiques d'une façon générale et dans les sciences naturelles.

1. *Groupes de Galois.* La théorie classique de Galois consiste dans l'application de la théorie des groupes à l'étude des corps commutatifs, réalisée d'une façon particulière que nous allons décrire. Soit K une extension finie, séparable, normale d'un corps commutatif k. Les automorphismes du corps K laissant fixes les éléments du sous-corps k forment un groupe G par rapport à leur exécution successive. Il s'appelle *groupe de Galois* de l'extension K/k. Le théorème fondamental de Galois dit qu'en associant à chaque sous-groupe $H \leqslant G$ son sous-corps fixe $K^H = \{x \mid x \in K,\ x^h = x$ pour tout $h \in H\}$,

on obtient une application anti-isomorphe du treillis des sous-groupes de G sur le treillis des sous-corps intermédiaires compris entre k et K. Une extension K^H/k sera encore finie, séparable, normale si et seulement si le sous-groupe H est normal dans G, auquel cas la restriction des automorphismes de G à K^H sera un homomorphisme de G sur le groupe de Galois de l'extension K^H/k de noyau H.

La théorie des groupes permet aussi de reconnaître si telle ou telle équation est résoluble ou non par radicaux. Soient f un polynôme de X sur un corps commutatif k et K le corps du développement de f. Soit G le groupe de Galois de l'extension K/k. Il s'appelle groupe de Galois du polynôme f sur le corps k (ses éléments se représentent naturellement par les permutations des racines de l'équation $f(X) = 0$). Le fait est que l'équation $f(X) = 0$ est résoluble par radicaux si et seulement si le groupe de Galois du polynôme f est polycyclique.

Une théorie parallèle à celle de Galois est celle de Picard-Vessiot qui étudie par les moyens de la théorie des groupes les extensions des anneaux différentiels et s'occupe en particulier de la résolubilité des équations différentielles par quadratures. Le rôle des groupes de permutations en théorie de Galois est joué en théorie de Picard-Vessiot par les groupes de matrices algébriques.

Dans ces exemples, les groupes interviennent sous forme de groupes d'automorphismes de structures mathématiques. En plus de son rôle fondamental, soulignons que cette forme d'application n'existe que pour les groupes, assurant à ces derniers une place privilégiée en algèbre. En effet, les automorphismes de structures quelconques se laissent toujours « grouper » (Galois), tandis qu'un anneau ou une autre structure quelconque ne se laisse définir sur l'ensemble des automorphismes que dans quelques cas spéciaux.

2. *Groupes d'homologie.* L'idée maîtresse de la théorie de l'homologie réside dans l'application de la théorie des groupes (abéliens) à l'étude de la catégorie des espaces topologiques. On fait correspondre à tout espace X une famille de groupes abéliens $H_0(X)$, $H_1(X)$, ... et à toute application continue $f: X \to Y$ une famille d'homomorphismes $f_n: H_n(X) \to H_n(Y)$, $n = 0, 1, 2, \ldots$ L'étude des groupes d'homologie $H_n(X)$ et de leurs homomorphismes par les moyens de la théorie des groupes permet bien souvent de résoudre le problème topologique de départ. Exemple: problème du prolongement. Une application $g: A \to Y$ définie sur un sous-espace A d'un espace X admet-elle un prolongement dans X tout entier, i.e. est-elle représentable par la composée d'une injection $h: A \to X$ et d'une application continue $\bar{g}: X \to Y$? Dans l'affirmative, il doit y avoir en homologies $g_n = \bar{g}_n h_n$, i.e. pour tout homomorphisme $g_n: H_n(A) \to H_n(Y)$ il existe un $H_n(X)$ avec un h_n donné. Si ce problème algébrique est irrésoluble, il est évident que le problème topologique de départ est sans solution, lui aussi.

Ce procédé donne d'excellents résultats. A titre d'illustration, donnons une esquisse de la démonstration du théorème de Brauer sur le point fixe : toute application f d'une boule E^n de dimension n dans elle-même admet un point fixe. Soit au contraire $f(x) \neq x$ pour tout $x \in E^n$. Menons par x une demi-droite issue de $f(x)$ et supposons qu'elle perce la sphère S^{n-1} en $\bar{g}(x)$. De toute évidence, $\bar{g}$ est continue, si bien que le problème du prolongement de l'application identique $g: S^{n-1} \to S^{n-1}$ en application $E^n \to S^{n-1}$ est résoluble. Pour $n = 1$, on a tout de suite une contradiction. Soit $n \geqslant 2$. Considérons une théorie d'homologie à coefficients dans $\mathbb{Z}$ (le groupe des entiers relatifs). On a $H_{n-1}(E^n) = 0$, $H_{n-1}(S^{n-1}) = \mathbb{Z}$, $h_{n-1} = 0$, $g_{n-1} = 1$. Il est clair que le problème algébrique auxiliaire n'a pas de solution, d'où une nouvelle contradiction.

Les groupes d'homologie illustrent un autre champ d'application typique des groupes : l'étude des objets non algébriques à l'aide des structures algébriques qui régissent le comportement de ces objets. Telle est en particulier la méthode fondamentale utilisée en topologie algébrique. Remarquons d'ailleurs qu'une méthode analogue et, en particulier, la méthode des groupes d'homologie est utilisée avec succès pour l'étude des structures algébriques elles-mêmes, par exemple dans la théorie des extensions de groupes.

3. *Groupes de symétrie.* Nous avons déjà dit que la notion de groupe permet d'évaluer en termes précis la propriété de symétrie de telle ou telle figure géométrique. C'est dans cet esprit que E. S. Fédorov (1890) a établi une classification des systèmes de points régulièrement disposés dans l'espace, un des problèmes clés de la cristallographie. Sur le plan, les groupes de Fédorov sont au nombre de dix-sept, ils ont tous été trouvés directement. Dans l'espace, il y en a 230 ; leur classification exhaustive ne fut possible que grâce à la théorie des groupes. Dans l'histoire des sciences naturelles, c'est le premier exemple d'application directe de la théorie des groupes.

En physique, la théorie des groupes joue un rôle analogue. Par exemple, en mécanique quantique, l'état d'un système physique est représenté par un point dans un espace vectoriel de dimension infinie. Au moment où le système change d'état, une transformation linéaire s'opère sur le point représentatif. Les raisons de symétrie et la théorie des représentations des groupes par les transformations linéaires y jouent un rôle de premier plan.

Les exemples précédents illustrent le rôle classifiant de la théorie des groupes dans tous les cas où il s'agit de caractériser une symétrie. Chaque fois que l'on a affaire à une symétrie, on a en fait affaire à des automorphismes de structures (non forcément mathématiques), si bien que l'importance de la théorie des groupes ne risque pas d'être surestimée. Dans les mathématiques mêmes, son rôle classifiant est important : il suffit de se rappeler le *Programme d'Erlangen* de Klein.

La notion de groupe, qui se trouve à la base des mathématiques contemporaines, constitue donc un outil polyvalent dans les mathématiques elles-mêmes: c'est la clé de voûte de toute une série de structures algébriques compliquées, un indicateur extrasensible des propriétés des différents êtres topologiques, un banc d'essai pour les algorithmes ... D'autre part, la notion de groupe est un puissant instrument d'exploration de l'une des lois les plus profondes de la Nature: la symétrie.

Passons en revue quelques grandes classes de groupes.

La branche la plus ancienne chronologiquement de la théorie des groupes, et qui reste néanmoins en évolution intense, est la théorie des groupes finis. Une place de choix y est occupée par la recherche des groupes finis simples parmi lesquels on trouve beaucoup de groupes classiques de matrices sur un corps commutatif fini, plusieurs séries de groupes d'automorphismes d'algèbres de Lie, ainsi que quelques groupes « sporadiques ». A l'autre pôle se trouvent les groupes finis résolubles dont certains sous-groupes spécifiques (de Hall, de Carter, etc.) font l'objet d'un intérêt soutenu, car ils déterminent dans une large mesure la structure du groupe lui-même. Dans bien des cas, les groupes finis apparaissent sous forme de groupes de permutations ou de matrices sur un corps fini: toute une branche de la théorie des groupes finis est réservée à l'étude des représentations par les matrices et les permutations.

Une méthode très usitée d'étude des groupes infinis consiste à leur imposer des conditions de finitude. L'intérêt le plus vif est suscité par les groupes périodiques, les groupes localement finis, les groupes artiniens, les groupes nœthériens, les groupes de type fini, les groupes de rang fini, les groupes résiduellement finis.

Parmi les groupes abéliens, on s'intéresse surtout aux groupes abéliens divisibles, aux groupes abéliens sans torsion et aux groupes abéliens périodiques, et dans ces derniers, aux sous-groupes purs et primaires. L'étude d'un groupe abélien quelconque se réduit dans bien des cas aux théories des classes indiquées par les moyens de la théorie des extensions des groupes abéliens, développée généralement par des méthodes d'homologie.

Plus larges encore que la classe des groupes abéliens, sont les classes des groupes nilpotents et résolubles, dont la théorie est aujourd'hui assez étoffée. Parmi les généralisations de la nilpotence et de la résolubilité, notons la nilpotence locale, la résolubilité locale, la condition du normalisateur, les groupes d'Engel, ainsi que de nombreuses classes de groupes définies par l'existence de telle ou telle structure normale à l'intérieur du groupe.

Enfin, en introduisant dans le groupe telle ou telle structure supplémentaire compatible avec sa loi de composition on obtient d'autres grandes divisions de la théorie des groupes: groupes topologiques, groupes de Lie, groupes algébriques, groupes linéaires.

CHAPITRE PREMIER

DÉFINITION ET PARTIES PRINCIPALES D'UN GROUPE

§ 1. Définition d'un groupe

1. 1. Axiomatique. Isomorphisme. Les ensembles et les fonctions sur les ensembles: voilà deux types d'objets dont s'occupe, en fin de compte, toute théorie mathématique. Si les arguments d'une fonction f parcourent un ensemble M et la fonction prend ses valeurs dans M, on dit que f est une *opération algébrique* sur M. La science qui étudie les opérations algébriques s'appelle *algèbre*. Elle ne s'intéresse pas du tout à l'objet de l'opération algébrique mais uniquement à sa façon d'agir. On fait abstraction de l'objet et l'on concentre son attention sur la façon d'agir de l'opération en faisant appel à la notion d'isomorphisme.

Soient deux ensembles munis d'opérations algébriques. Supposons qu'il existe une correspondance biunivoque entre les ensembles eux-mêmes et entre les ensembles d'opérations définies sur ces derniers, les opérations correspondantes étant fonctions d'un même nombre d'arguments et prenant des valeurs correspondantes pour des valeurs correspondantes d'arguments. On dit alors que ces ensembles munis d'opérations sont *isomorphes*.

Les objets isomorphes ont même structure vis-à-vis des opérations, si bien qu'on ne fait aucune distinction en algèbre entre les objets isomorphes, ou bien on les considère comme des copies exactes, de la même façon que nous ne faisons aucune distinction entre deux exemplaires d'un même roman, bien que composés en caractères différents et imprimés sur papier différent, si nous ne nous intéressons qu'au contenu du roman. Il est rationnel de considérer que chaque classe d'objets isomorphes fait ressortir clairement un type déterminé d'opération algébrique. Le problème de l'algèbre — étude des opérations algébriques — s'en trouve réduit à une tâche plus concrète, celle d'étude des ensembles munis d'opérations à isomorphisme près.

Certaines opération salgébriques sont si fréquentes en mathématiques qu'elles font l'objet de théories indépendantes. C'est précisément le cas du groupe, objet de la théorie des groupes. Un groupe est un ensemble muni d'une opération binaire (à deux éléments) régie par certains axiomes. Au lieu de noter la valeur de l'opération

l inaire f sur un couple d'éléments x, y sous la forme $f(x, y)$ comme pour les autres opérations, nous écrirons simplement xfy : cela fait trois symboles en moins. En outre, cette notation est conforme à l'écriture canonique des opérations sur les nombres : en effet, nous écrivons bien $2 + 3 = 5$ et non $+(2, 3) = 5$. En théorie des groupes, l'opération binaire est généralement appelée multiplication et notée par un point (omis le plus souvent) ; quelquefois elle est notée par $+$, $\circ$, $*$ ou par d'autres symboles. L'écriture avec un point s'appelle aussi notation multiplicative, et avec un $+$, notation additive.

1.1.1. Définition. Un ensemble G muni d'une opération binaire $\cdot$ s'appelle *groupe* si :

1. L'opération est *associative*, i.e. $(ab)c = a(bc)$ pour a, b, c quelconques appartenant à G.
2. L'opération garantit l'unité, i.e. il existe dans G un élément e, appelé *élément neutre* ou *unité*, tel que $ae = ea = a$ pour tout a appartenant à G.
3. L'opération garantit les éléments inverses, i.e. pour tout a appartenant à G il existe dans G un élément x, appelé *inverse* de a, tel que $ax = xa = e$.

1.1.2. Définition. Un ensemble G muni d'une opération binaire $\cdot$ s'appelle groupe si :

1. L'opération est associative.
2. L'opération garantit les quotients à gauche et à droite, i.e. pour deux éléments quelconques a, b de G il existe dans G des éléments x, y, appelés respectivement *quotient à gauche* et *quotient à droite* de b par a, tels que $ax = b$, $ya = b$.

1.1.3. Exercice. Les définitions 1.1.1 et 1.1.2 sont équivalentes. Il n'y a qu'une seule unité dans n'importe quel groupe G. Tout élément a de G admet un seul inverse, noté a^{-1}. Pour deux éléments quelconques a, b de G les deux quotients de b par a sont uniques (notations : $a \setminus b$, quotient à gauche ; b/a, quotient à droite).

En accord avec la conception générale d'isomorphisme, une bijection φ d'un groupe sur un autre, conservant le produit, est dite *isomorphe*. Autrement dit, une application φ d'un groupe G dans un groupe G^* (notations $\varphi : G \to G^*$) est isomorphe si les éléments distincts admettent des images distinctes (l'image d'un élément a par l'application φ est notée a^φ),

$$a^\varphi \neq b^\varphi \text{ pour } a \neq b \quad (a, b \in G),$$

et l'image du produit est égale au produit des images,

$$(ab)^\varphi = a^\varphi b^\varphi.$$

Deux groupes sont *isomorphes* (notation $G \simeq G^*$) s'il existe un isomorphisme d'un groupe *sur* l'autre.

Par exemple, l'ensemble G de nombres réels strictement positifs est un groupe par rapport à la multiplication ordinaire des nombres; l'ensemble G^* de tous les nombres réels est un groupe par rapport à l'addition ordinaire des nombres; l'application $\varphi : G \to G^*$ définie par la formule $a^\varphi = \log a$ est un isomorphisme de G sur G^*. Nous profitons de cet isomorphisme quand nous nous servons d'une règle à calcul (on dit d'ailleurs aussi règle logarithmique).

L'objet de la théorie des groupes est l'étude des lois de composition interne ou, en d'autres termes, l'étude des groupes à isomorphisme près. La théorie des groupes serait achevée s'il était possible de dresser un catalogue exhaustif des groupes à isomorphisme près. Heureusement pour la théorie des groupes et malheureusement pour les applications, un tel catalogue est pratiquement impossible à établir.

1.2. Exemples. L'opération étant associative dans le groupe, un élément $(ab)\,c = a\,(bc)$ peut se noter simplement abc. Pour la même raison, un produit de n éléments $a_1 a_2 \ldots a_n$ est défini de façon unique dans le groupe, sans parenthèses, à condition que l'ordre indiqué soit conservé. Le produit de n éléments égaux à a est appelé *puissance n-ième* de a et est noté a^n. On pose ensuite $a^0 = e$; pour $n < 0$, on a $a^n = (a^{-n})^{-1}$ ou $a^n = (a^{-1})^{-n}$, ce qui revient évidemment au même.

1.2.1. Exercice. Si a est un élément quelconque du groupe et m, n sont deux entiers relatifs, alors $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

On a parfois $a^n = e$ pour un $n > 0$: le plus petit n vérifiant cette condition s'appelle alors *ordre* ou *période* de l'élément a et se note $|a|$. Si $a^n \neq e$ pour aucun $n > 0$, on dit que a est d'ordre infini et l'on écrit $|a| = \infty$.

1.2.2. Exercice. Si $a^n = e$, alors n est divisible par $|a|$.

1.2.3. Exercice. Si deux éléments a, b commutent (ou sont permutables), i.e. $ab = ba$, et si leurs ordres sont premiers entre eux, on a $|ab| = |a| \cdot |b|$.

1.2.4. Exercice. Soient deux éléments permutables a, b d'ordres respectifs m, n. Il existe alors dans le groupe un élément — qui n'est déjà pas nécessairement le produit ab — dont l'ordre est le ppcm de m et n.

On dit que le groupe G est *sans torsion* (ou *apériodique*) si tous ses éléments non triviaux (autres que l'unité) sont d'ordre infini. Au contraire, si tous les éléments sont d'ordre fini, on dit que le groupe est *périodique*. Un groupe qui contient des éléments non triviaux d'ordres finis et infinis est dit *mixte*. Si les ordres des éléments d'un

groupe périodique sont bornés dans leur ensemble, leur ppcm s'appelle *période* ou *exposant* du groupe.

Soit p un nombre premier. Un groupe périodique dont les ordres des éléments sont des puissances de p s'appelle *p-groupe*. Les groupes qui sont des p-groupes pour un p premier quelconque sont appelés *groupes primaires*. Le cardinal $|G|$ d'un groupe G s'appelle *ordre* de G. Si ce cardinal est fini, le groupe G est dit *fini*, et *infini* dans le cas contraire. Si l'opération sur G est commutative, i.e. $ab = ba$ pour deux éléments quelconques a, b de G, on dit que G est un *groupe commutatif*, ou *abélien*, du nom du mathématicien norvégien Niels Henrik Abel. Une opération commutative est souvent notée additivement. On utilise alors le petit dictionnaire suivant :

$\cdot$	$+$	$\cdot$	$+$
multiplication	addition	quotient	différence
produit	somme	e ou 1	0
unité	zéro	a^{-1}	$-a$
inverse	opposé	a^n	na
puissance	multiple	a/b, $b\backslash a$	$a-b$

Les groupes sont partout : théorie de Galois et théorie des équations différentielles, topologie algébrique et classification des particules élémentaires en physique, cristallographie et théorie de la relativité, théorie des nœuds, différentes autres branches de la topologie et de la théorie des fonctions, voici une liste bien incomplète des domaines de la science où intervient la notion de groupe ; intervenir ne veut pas dire ici se manifester gratuitement mais travailler avec application. De gros volumes ont été écrits pour cerner la portée de la théorie des groupes vis-à-vis des différentes sciences ; conseillant aux étudiants intéressés la lecture de ces traités, nous nous bornerons à citer quelques exemples dans le cadre du cours d'algèbre générale, cadre que nous nous sommes posé dans ce livre. (Les notations en caractères gras, dites notations canoniques, désigneront les mêmes êtres mathématiques jusqu'à la fin du livre. Ce sont des notations universellement admises, à quelques petites nuances près, dans la littérature ; nous en donnons une liste complète en page 6 afin de faciliter la lecture.)

1.2.5. Exemples. I. L'ensemble des éléments d'un anneau K est un groupe abélien par rapport à l'addition. Nous l'appellerons *groupe additif de l'anneau K* et nous le noterons par la même lettre K que l'anneau, conformément au principe selon lequel une lettre désigne un ensemble ; quant aux opérations définies sur l'ensemble, el-

les doivent être expliquées dans le contexte. En particulier, les groupes additifs du corps des nombres complexes $\mathbb{C}$, du corps des nombres réels $\mathbb{R}$, du corps des nombres rationnels $\mathbb{Q}$, de l'anneau des entiers relatifs $\mathbb{Z}$ sont des groupes abéliens sans torsion. D'une façon générale, le groupe additif d'un corps de caractéristique nulle est sans torsion, et le groupe additif d'un corps de caractéristique positive p est de période p. Les groupes additifs d'un corps fini $\mathbf{GF}(q)$ de q éléments et ceux de l'anneau $\mathbb{Z}_n$ des résidus modulo n sont des groupes abéliens finis, de telle sorte que

$$|\mathbf{GF}(q)| = q, \quad |\mathbb{Z}_n| = n.$$

Soit p un nombre premier. Un nombre rationnel de la forme m/p^n, avec m, n entiers relatifs, s'appelle *fraction p-aire*. L'ensemble $\mathbb{Q}_p$ de toutes les fractions p-aires, muni de l'addition ordinaire des nombres est un groupe abélien sans torsion.

II. L'ensemble de tous les éléments inversibles d'un anneau unitaire K est un groupe par rapport à la multiplication. Il s'appelle *groupe multiplicatif de l'anneau* K et se note K^* (si $|K| \geqslant 2$, l'ensemble K^* est toujours sans zéro, donc distinct de l'ensemble K). Si l'anneau K^* est commutatif, le groupe K^* l'est aussi. En particulier, les groupes multiplicatifs $\mathbb{C}^*$, $\mathbb{R}^*$, $\mathbb{Q}^*$, $\mathbb{Z}^*$, $\mathbf{GF}(q)^*$, $\mathbb{Z}_n^*$ sont abéliens. L'ensemble $\mathbb{C}_n$ des nombres complexes vérifiant l'équation $x^n = 1$ est un groupe abélien par rapport à la multiplication ordinaire des nombres. Soit p un nombre premier. L'ensemble $\mathbb{C}_{p^\infty}$ de toutes les racines de l'équation $x^{p^n} = 1$, $n = 1, 2, \ldots$, sur le corps des nombres complexes est un p-groupe abélien infini par rapport à la multiplication ordinaire. Il porte le nom de *groupe quasi cyclique du type* p^∞. Les groupes $\mathbb{Z}^*$, $\mathbf{GF}(q)^*$, $\mathbb{Z}_n^*$, $\mathbb{C}_n$ sont finis et

$$|\mathbb{Z}^*| = 2, \quad |\mathbf{GF}(q)^*| = q - 1, \quad |\mathbb{Z}_n^*| = \varphi(n),$$
$$|\mathbb{C}_n| = n,$$

où φ est la fonction d'Euler, i.e. $\varphi(mn) = \varphi(m)\varphi(n)$ quand m et n sont premiers entre eux et $\varphi(p^k) = p^k - p^{k-1}$ pour p premier.

III. Soient M un ensemble et $\mathbf{S}(M)$ l'ensemble des applications bijectives de M sur M. En prenant comme multiplication sur $\mathbf{S}(M)$ la réalisation successive des applications, $\mathbf{S}(M)$ devient un groupe. En particulier, pour $M = \{1, \ldots, n\}$ ce groupe devient le groupe des permutations de degré n. Il s'appelle alors *groupe symétrique* de degré n et se note $\mathbf{S}_n$. Le groupe $\mathbf{S}_n$ est fini et $|\mathbf{S}_n| = n!$. Pour $n > 2$, le groupe $\mathbf{S}_n$ est non abélien.

IV. L'ensemble $\mathbf{GL}_n(K)$ de toutes les matrices inversibles d'ordre n sur un anneau commutatif unitaire K est un groupe par rapport à la multiplication ordinaire des matrices. Il s'appelle *groupe linéaire général* ou *groupe matriciel général* de degré n sur l'anneau K. Il est évi-

dent que $\mathbf{GL}_n(K) = \mathbf{M}_n(K)^*$, où $\mathbf{M}_n(K)$ est l'anneau de toutes les matrices d'ordre n sur K. Pour $n \geqslant 2$, le groupe $\mathbf{GL}_n(K)$ est non abélien. Considérons ensuite dans $\mathbf{GL}_n(K)$ les parties suivantes: $\mathbf{SL}_n(K)$ des matrices de déterminant 1; $\mathbf{D}_n(K)$ des matrices diagonales; $\mathbf{T}_n(K)$ des matrices trigonales supérieures; $\mathbf{UT}_n(K)$ des matrices trigonales supérieures ayant des unités sur la diagonale. Tous les ensembles énumérés sont encore des groupes par rapport à la multiplication des matrices. Ils s'appellent respectivement: *groupe linéaire spécial*, *groupe diagonal*, *groupe trigonal*, *groupe unitrigonal*. Si l'on prend comme K un corps fini $\mathbf{GF}(q)$, on écrit $\mathbf{GL}_n(q)$ au lieu de $\mathbf{GL}_n(K)$; les autres groupes matriciels sont notés de façon analogue.

1.2.6. Exercice. $\mathbb{Z}_n \simeq \mathbb{C}_n$.

1.2.7. Exercice. Le groupe $\mathbf{C}^*$ est isomorphe au groupe de toutes les matrices non dégénérées de la forme $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ à coefficients réels, par rapport à la multiplication ordinaire des matrices.

1.2.8. Exercice. $\mathbb{Q}_p \not\simeq \mathbb{Q}_q$ pour $p \neq q$.

1.2.9. Exercice. Si une permutation a de $\mathbf{S}_n$ peut être mise sous la forme d'un produit de cycles indépendants de longueur $n_1, \ldots, n_k$, son ordre $|a|$ est égal au ppcm des $n_1, \ldots, n_k$.

On peut augmenter à volonté le nombre des exemples de groupes en se donnant un procédé susceptible de former des groupes nouveaux à partir des groupes donnés. La théorie des groupes connaît de très nombreux procédés de ce type. Voici un procédé très simple mais important.

Soient $G_1, \ldots, G_m$ des groupes. Il est facile de voir que l'ensemble $G = G_1 \times \ldots \times G_m$ des suites $\langle g_1, \ldots, g_m \rangle$, $g_\alpha \in G_\alpha$, muni de la multiplication composante par composante

$$\langle g_1, \ldots, g_m \rangle \cdot \langle g'_1, \ldots, g'_m \rangle = \langle g_1 g'_1, \ldots, g_m g'_m \rangle$$

est un groupe. On l'appelle *produit cartésien* des groupes G_α, et les groupes G_α, ses *facteurs*. Cette notion s'étend sans peine au cas d'un ensemble arbitraire de facteurs G_α, $\alpha \in I$. En effet, désignons par

$$G = \prod_{\alpha \in I} G_\alpha$$

l'ensemble des fonctions

$$f : I \to \bigcup_{\alpha \in I} G_\alpha$$

telles que $f(\alpha) \in G_\alpha$ pour tout $\alpha \in I$. On voit sans peine que l'ensemble G muni de la multiplication $(fg)(\alpha) = f(\alpha)\, g(\alpha)$ est un groupe; on l'appelle *produit cartésien* des groupes G_α. La valeur prise par la

fonction f en α s'appelle *projection* ou *composante* de f dans le facteur G_α. L'ensemble

$$\operatorname{supp}(f) = \{\alpha \mid \alpha \in I,\ f(\alpha) \neq e\}$$

s'appelle *support* de la fonction f. Il est clair que l'ensemble des fonctions aux supports finis, qui interviennent au produit cartésien des groupes G_α, est encore un groupe par rapport à la multiplication des fonctions. Il s'appelle *produit direct* des groupes G_α et se note $\prod_{\alpha \in I} G_\alpha$ (sans barre). Il est clair que le produit direct et le produit cartésien se confondent quand les facteurs sont en nombre fini.

L'opération d'un groupe étant écrite en notation additive, on dit *somme* au lieu de produit et *terme* (ou *sommant*) au lieu de facteur et l'on écrit

$$G = G_1 \oplus \ldots \oplus G_m,$$

$$G = \sum_{\alpha \in I} G_\alpha, \quad G = \overline{\sum_{\alpha \in I}} G_\alpha.$$

1.2.10. Exercice. $\mathbb{C}_m \times \mathbb{C}_n \simeq \mathbb{C}_{mn}$ pour m, n premiers entre eux.

1.2.11. Exercice. $\mathbb{D}_n(K) \simeq K^* \times \ldots \times K^*$ (n fois).

1.2.12. Exercice. Soit a l'élément d'ordre fini n d'un groupe. Faisons une décomposition canonique de n en facteurs premiers

$$n = \prod_p p^{m(p)}$$

et posons $n_p = n/p^{m(p)}$. L'élément a^{n_p} est d'ordre $p^{m(p)}$; il existe des entiers x_p tels que

$$a = \prod_p a^{n_p x_p}.$$

§ 2. Sous-groupes. Le sous-groupe normal

2.1. Sous-groupes. Si une partie H d'un groupe G est fermée par rapport à la multiplication, i.e. si elle contient pour ses deux éléments quelconques a, b leur produit ab, la restriction de la multiplication à H sera une opération algébrique sur H ; on dit que cette opération est *induite* par la multiplication dans G. Si H est un groupe par rapport à l'opération induite, on dit que H est un *sous-groupe* de G et l'on écrit $H \leqslant G$. Si $H \leqslant G$ et $H \neq G$, on écrit $H < G$ (ne pas confondre avec les symboles d'inclusion d'ensembles $\subseteq$, $\subset$!).

2.1.1. Exercice. Pour que la partie H d'un groupe G soit un sous-groupe, il faut et il suffit que H soit fermée par rapport à la multiplication et à l'inversion, i.e. que, pour ses deux éléments

quelconques a, b, elle contienne aussi ab et a^{-1}. Ces conditions de fermeture peuvent s'écrire également

$$HH \subseteq H, \quad H^{-1} \subseteq H$$

en faisant intervenir les notations usuelles

$$AB = \{ab \mid a \in A,\ b \in B\}, \qquad A^{-1} = \{a^{-1} \mid a \in A\}$$

pour deux parties quelconques A, B du groupe donné.

2.1.2. Exercice. Le produit AB de deux sous-groupes A, B d'un groupe G est lui-même un sous-groupe si et seulement si $AB = BA$.

2.1.3. Exercice. Si A, B sont deux sous-groupes finis, on a

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Dans tout groupe, l'ensemble réduit à l'unité et le groupe tout entier sont des sous-groupes. Tous les sous-groupes autres que le sous-groupe unité et le groupe tout entier s'appellent *propres* ou *vrais* ou *véritables*.

Continuons l'étude des groupes I à IV du § 1 et indiquons quelques sous-groupes dans ces groupes.

2.1.4. Exemples. I. On a évidemment

$$\mathbb{Z} < \mathbb{Q}_p < \mathbb{Q} < \mathbb{R} < \mathbb{C},$$
$$\mathbb{Z} = \bigcap \mathbb{Q}_p,$$
$$\mathrm{GF}\ (p^m) \leqslant \mathrm{GF}\ (p^n) \text{ pour } m \mid n.$$

II. Il est évident que

$$\mathbb{Z}^* < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*,$$
$$\mathbb{C}_p < \mathbb{C}_{p^2} < \ldots < \mathbb{C}_{p^\infty},$$
$$\mathbb{C}_{p^\infty} = \bigcup \mathbb{C}_{p^n},$$
$$\mathrm{GF}\ (p^m)^* \leqslant \mathrm{GF}\ (p^n)^* \quad \text{pour } m \mid n.$$

III. Dans le groupe symétrique S_n, l'ensemble A_n de toutes les permutations paires est un sous-groupe. Il s'appelle *groupe alterné* de degré n. On a évidemment $|\mathrm{A}_n| = \frac{1}{2} n!$.

IV. Pour $n \geqslant 2$, on a

$$\mathrm{SL}_n\ (K) \leqslant \mathrm{GL}_n\ (K),$$
$$\mathrm{D}_n\ (K) < \mathrm{T}_n\ (K),$$
$$\mathrm{UT}_n\ (K) \leqslant \mathrm{T}_n\ (K) < \mathrm{GL}_n\ (K).$$

Indiquons aussi dans $\mathbf{GL}_n(K)$ le sous-groupe *orthogonal*

$$\mathbf{O}_n(K) = \{a \mid aa' = e\}$$

(la prime désigne la transposition), et pour $K = \mathbb{C}$ aussi le groupe *unitaire*

$$\mathbf{U}_n = \{a \mid a\bar{a}' = e\}$$

(la barre désigne le passage au conjugué complexe de chaque élément de la matrice). Enfin,

$$\mathbf{UT}_n(K) = \mathbf{UT}_n^1(K) \geqslant \mathbf{UT}_n^2(K) \geqslant \ldots,$$

où $\mathbf{UT}_n^m(K)$ est l'ensemble des matrices de $\mathbf{UT}_n(K)$ qui ont $m-1$ diagonales nulles au-dessus de la diagonale principale.

2.2. Ensembles générateurs. Il est facile de voir que l'intersection d'une famille de sous-groupes est un sous-groupe. Si M est une partie d'un groupe G, l'intersection (M) de tous les sous-groupes contenant M est appelée sous-groupe *engendré* par M, ce dernier étant appelé *ensemble générateur* de (M). On dit parfois par abus de langage que les éléments de M sont les *éléments générateurs* de (M). Le sous-groupe (M) se note aussi gr (M), ce qui est surtout utile dans les formules encombrantes. Un groupe engendré par un ensemble fini s'appelle *groupe à engendrement fini* ou *groupe de type fini*. Plus généralement et plus exactement, on dit que le groupe est $\mathfrak{m}$-*engendré* si son ensemble générateur est de cardinal $\mathfrak{m}$.

2.2.1. Théorème. *Si M est une partie de G, on a*

$$(M) = \{a_1^{\varepsilon_1} \ldots a_m^{\varepsilon_m} \mid a_i \in M, \quad \varepsilon_i = \pm 1, \ m = 1, 2, \ldots\}.$$

Démonstration. Désignons le second membre par H. Puisque le sous-groupe (M) contient tous les a_i de M, on a $(M) \supseteq H$. D'autre part, $HH \subseteq H$, $H^{-1} \subseteq H$, aussi H est-il un sous-groupe contenant M, d'où $H \supseteq (M)$ et définitivement $H = (M)$.

A titre d'illustration, indiquons les ensembles générateurs des groupes I à IV du § 1. Nous écrirons

$$(M) = (\ldots \mid \ldots)$$

si M est défini sous la forme

$$M = \{\ldots \mid \ldots\},$$

i.e. nous omettrons les accolades à l'intérieur des parenthèses.

2.2.2. Exemples. I. Il est évident que

$$\mathbb{Z} = (1),$$
$$\mathbb{Z}_n = (1 \pmod{n}),$$
$$\mathbb{Q} = \left(\frac{1}{n} \,\middle|\, n = 1, 2, \ldots\right).$$

II. Il est évident que

$$\mathbb{Z}^* = (-1),$$
$$\mathbb{Q}^* = (-1, 2, 3, 5, 7, 11, \ldots),$$
$$\mathrm{GF}\,(q)^* = (\zeta_q),$$
$$\mathbb{C}_n = (\alpha_n),$$
$$\mathbb{C}_{p^\infty} = (\alpha_{p^m} \mid m = 1, 2, \ldots),$$

où ζ_q est racine primitive de l'équation $x^{q-1} = 1$ sur le corps GF (q),

$$\alpha_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

III. On apprend dans le cours d'algèbre générale que le groupe symétrique $\mathbf{S}_n$ est engendré par ses transpositions (ij). Puisque $(ij) = (1i)\,(1j)\,(1i)$, le groupe $\mathbf{S}_n$ est engendré même par les transpositions (12), (13), . . ., $(1n)$. Le groupe alterné $\mathbf{A}_n$ est engendré par les différents cycles à trois éléments (ijk), car une permutation paire est le produit d'un nombre pair de transpositions et

$$(ij)\,(ik) = (ijk),\ (ij)\,(kl) = (ilj)\,(jkl).$$

IV. Soit K un corps commutatif. Considérons dans $\mathbf{GL}_n\,(K)$ des matrices de la forme

$$t_{ij}\,(\alpha) = e + \alpha e_{ij},\ d\,(\beta) = e + (\beta - 1)\,e_{nn},$$
$$\alpha,\ \beta \in K,\quad \beta \neq 0,\quad i \neq j,$$

où e est la matrice unité et e_{ij} une matrice ayant un 1 en position (i, j) et des 0 dans les autres positions. Pour $\alpha \neq 0$, les matrices $t_{ij}\,(\alpha)$ s'appellent *transvections*. Montrons que toute matrice dans $\mathbf{GL}_n\,(K)$ se laisse mettre sous la forme

$$t_1 \ldots t_r d\,(\beta)\, t_{r+1} \ldots t_s,$$

où t_i sont des transvections. Cela revient à dire en particulier que

$$\mathbf{GL}_n\,(K) = (t_{ij}\,(\alpha),\ d\,(\beta) \mid \alpha,\ \beta \in K,\quad i \neq j), \tag{1}$$
$$\mathbf{SL}_n\,(K) = (t_{ij}\,(\alpha) \mid \alpha \in K,\quad i \neq j). \tag{2}$$

En effet, multiplier la matrice par une transvection à droite revient à ajouter à une de ses colonnes une autre colonne multipliée par un scalaire de K; la multiplier par une transvection à gauche

revient à faire une transformation analogue sur ses lignes; de pareilles transformations seront appelées *élémentaires*. Soit $a \in \mathrm{GL}_n(K)$. En opérant des transformations élémentaires sur les colonnes de la matrice a, on peut faire en sorte que $a_{12} \neq 0$. Une nouvelle transformation élémentaire, qui consiste à ajouter à la première colonne une deuxième colonne multipliée par $\frac{1-a_{11}}{a_{12}}$, nous permet d'obtenir 1 en position (1, 1), puis d'obtenir des 0 dans la première ligne et dans la première colonne de la matrice, à l'exception de la position (1, 1) où nous laissons 1. Poursuivant ce processus relativement au bloc inférieur de droite d'ordre $n - 1$, nous aboutirons finalement à une matrice du type $d(\beta)$. On a donc $a = t_1 \ldots t_r d(\beta)\, t_{r+1} \ldots t_s$, où t_i sont des transvections, ce qu'il fallait démontrer.

On démontre d'une façon analogue que

$$\mathrm{T}_n(K) = (t_{ij}(\alpha),\ \mathrm{diag}(\beta_1 \ldots, \beta_r) \mid \alpha,\ \beta \in K,\quad i < j), \tag{3}$$

$$\mathrm{UT}_n^m(K) = (t_{ij}(\alpha) \mid \alpha \in K,\quad j - i \geqslant m). \tag{4}$$

Les résultats obtenus permettent de déterminer $\mathrm{SL}_n(K)$ sur des anneaux K non commutatifs pour lesquels la notion de déterminant ordinaire n'a pas de sens. A cet effet, on prend comme définition pour les anneaux de ce type la formule (2). Soit ensuite K un corps. En analogie parfaite avec ce qui précède, toute matrice inversible a sur K se laisse mettre sous la forme $a = t_1 \ldots t_r d(\beta)\, t_{r+1} \ldots \ldots t_s$, $\beta \neq 0$. Pour les lecteurs initiés aux notions de commutant et de groupe quotient, notons que l'image de β par passage au quotient de K^* par le commutant s'appelle *déterminant de la matrice a au sens de Dieudonné*.

2.2.3. Exercice. Soient $n \geqslant 2$, $p_1, \ldots, p_n$ des nombres premiers distincts, $\bar{p}_i = p_1 \ldots p_{i-1} p_{i+1} \ldots p_n$. Alors

$$\mathbb{Z} = \mathrm{gr}(\bar{p}_1, \ldots, \bar{p}_n)$$

sans qu'il soit possible d'éliminer un seul élément de cet ensemble générateur.

2.2.4. Exercice. $\mathrm{S}_n = \mathrm{gr}((12), (12 \ldots n))$.

2.2.5. Exercice.

$$\mathrm{SL}_n(\mathbb{Z}) = \mathrm{gr}(e + e_{ij} \mid 1 \leqslant i \leqslant n,\quad 1 \leqslant j \leqslant n,\quad i \neq j),$$

$$\mathrm{SL}_n(\mathbb{Z}) = \mathrm{gr}(e + e_{12},\ e_{12} + e_{23} + \ldots + e_{n-1,\,n} + (-1)^{n-1} e_{n1}).$$

L'antipode des ensembles générateurs est le sous-groupe de Frattini. Pour définir cette notion, nous dirons qu'un sous-groupe H d'un groupe G est son *sous-groupe maximal par rapport à la propriété* σ si H possède la propriété σ et s'il n'existe dans G aucun sous-groupe possédant σ et contenant H. Si σ est la propriété d'être plus petit que G, les sous-groupes maximaux par rapport à σ sont dits

maximaux tout court. Il se peut bien sûr que le groupe soit sans sous-groupe maximal, cf. les exemples ci-après. Par définition, le *sous-groupe de Frattini* $\Phi(G)$ du groupe G est l'intersection de tous ses sous-groupes maximaux s'ils existent, et le groupe G lui-même dans le cas contraire.

Nous disons que x est un *élément non générateur* du groupe G s'il est possible de l'éliminer de n'importe quel ensemble générateur de G dont il fait partie.

2.2.6. Théorème. *L'ensemble S de tous les éléments non générateurs d'un groupe G se confond avec le sous-groupe de Frattini $\Phi(G)$.*

Démonstration. a) $S \subseteq \Phi(G)$. En effet, si G n'admet aucun sous-groupe maximal, l'assertion est triviale. Soient maintenant $x \in S$ et H un sous-groupe maximal dans G. Si $x \notin H$, on a $(x, H) = G$, $(H) \neq G$, contradiction avec $x \in S$. On a donc $x \in H$, $x \in \Phi(G)$.

b) $\Phi(G) \subseteq S$. Supposons par absurde qu'il existe un élément $x \in \Phi(G)$ qui, avec un ensemble M, $(M) \neq G$, engendre le groupe G. En vertu du lemme de Zorn, il existe des sous-groupes H maximaux parmi les sous-groupes contenant M et ne contenant pas x. Il est clair que ces sous-groupes sont maximaux tout court. Or, ils contiennent alors $\Phi(G)$, donc aussi x, contradiction. Le théorème est démontré.

2.2.7. Exemples. I. Dans le groupe $\mathbb{Z}$, le sous-groupe (p) est maximal pour p premier quelconque, aussi $\Phi(\mathbb{Z}) = 0$. On comprend sans peine que tout élément dans $\mathbb{Q}$ est non générateur, aussi $\Phi(\mathbb{Q}) = \mathbb{Q}$.

II. Puisque le groupe $\mathbb{C}_{p^\infty}$ se confond avec le réunion des sous-groupes $\mathbb{C}_{p^n}$, $n = 1, 2, \ldots$, chacun de ses éléments est non générateur. On a donc $\Phi(\mathbb{C}_{p^\infty}) = \mathbb{C}_{p^\infty}$.

III. On vérifie que le sous-groupe H_i du groupe $\mathbf{S}_n$, constitué par toutes les permutations laissant i invariant, est maximal dans $\mathbf{S}_n$. Puisque l'intersection $H_1 \cap \ldots \cap H_n$ est égale à 1, on a $\Phi(\mathbf{S}_n) = 1$. On montre de même que $\Phi(\mathbf{A}_n) = 1$.

IV. Considérons dans le groupe $\mathbf{UT}_n(\mathbb{Z})$ le sous-groupe H_{ip} constitué par toutes les matrices x telles que $x_{i,i+1} \in (p)$, où $1 \leqslant i \leqslant n-1$, p premier. On montre que H_{ip} est maximal dans $\mathbf{UT}_n(\mathbb{Z})$. Puisque l'intersection de tous les H_{ip} est contenue dans $\mathbf{UT}_n^2(\mathbb{Z})$, on a $\Phi(\mathbf{UT}_n(\mathbb{Z})) \leqslant \mathbf{UT}_n^2(\mathbb{Z})$. En fait, on démontre aussi l'inclusion inverse, i.e.

$$\Phi(\mathbf{UT}_n(\mathbf{Z})) = \mathbf{UT}_n^2(\mathbf{Z}).$$

2.3. Groupes cycliques et localement cycliques. Rang. Un sous-groupe (a) engendré par un élément unique a s'appelle *cyclique*.

En vertu du théorème 2.2.1, il réunit toutes les puissances possibles de l'élément générateur :

$$(a) = \{a^n \mid n = 0, \pm 1, \pm 2, \ldots\}.$$

L'exemple 2.2.2. I montre que $\mathbb{Z}$ et $\mathbb{Z}_n$ sont des groupes cycliques. Il se trouve qu'il n'existe aucun groupe cyclique — à isomorphisme près — en dehors de ces deux groupes.

2.3.1. Théorème. *Tout groupe cyclique infini est isomorphe au groupe $\mathbb{Z}$, tout groupe cyclique d'ordre fini n est isomorphe au groupe $\mathbb{Z}_n$.*

Démonstration. Soit (a) un groupe cyclique infini. Donnons-nous une application φ: $\mathbb{Z} \to (a)$ en posant $n^\varphi = a^n$. Elle est biunivoque : si l'on avait $n^\varphi = m^\varphi$ pour $n > m$, i.e. $a^{n-m} = e$, le groupe (a) serait fini. Par ailleurs, $(n + m)^\varphi = n^\varphi m^\varphi$, i.e. φ est un isomorphisme. Si (b), (c) sont deux groupes cycliques d'ordre fini n, on a un isomorphisme de (b) sur (c) en posant $b^k \mapsto c^k$, $0 \leqslant k \leqslant n - 1$.

2.3.2. Théorème. *Tout sous-groupe d'un groupe cyclique est un groupe cyclique.*

Démonstration. Soient (a) un groupe cyclique d'ordre n et H son sous-groupe quelconque autre que 1 (le sous-groupe unité est évidemment cyclique). Soit m le plus petit entier tel que

$$a^m \in H, \ 0 < m < n.$$

On a évidemment $(a^m) \subseteq H$. Montrons qu'on a en réalité $(a^m) = H$. Choisissons dans H un élément quelconque de la forme a^k, où $0 \leqslant k < n$. Divisons k par m avec reste, $k = mq + r$, $0 \leqslant r < m$. Il vient

$$a^r = a^k (a^m)^{-q} \in H.$$

En vertu du choix de m et de r, il en découle que $r = 0$ et $a^k \in (a^m)$. On montre d'une façon analogue que tout sous-groupe d'un groupe cyclique infini est un groupe cyclique.

On dit que le groupe est *localement cyclique* si chacune de ses parties finies engendre un sous-groupe cyclique.

2.3.3. Exercice. Montrer que $\mathbb{Q}$ et $\mathbb{Q}_{p^\infty}$ sont des groupes localement cycliques. En particulier, ils n'admettent aucun ensemble générateur fini.

D'une façon plus générale, nous dirons qu'un groupe G est *localement* $\mathfrak{m}$*-engendré* si chacun de ses sous-groupes de type fini est $\mathfrak{n}$-engendré pour un $\mathfrak{n} \leqslant \mathfrak{m}$. Le plus petit cardinal $\mathfrak{m}$ possédant cette propriété s'appelle le *rang* de G. Il est clair que le rang d'un groupe

est toujours soit fini, soit dénombrable (auquel cas il est noté par le symbole ∞). Ainsi donc, les groupes localement cycliques sont tous de rang 1. Il va sans dire que le rang du groupe n'est jamais supérieur à son cardinal et que le rang du sous-groupe n'est jamais supérieur à celui du groupe.

2.3.4. Exercice. Si G est produit direct de p-groupes G_p pour différents p premiers parcourant un ensemble π, on a

$$\operatorname{rang} G = \sup_{p \in \pi} (\operatorname{rang} G_p).$$

Indication. Voir 1.2.12.

2.4. Classes suivant un sous-groupe. A chaque sous-groupe H d'un groupe G on peut associer des ensembles

$$gH = \{gh \mid h \in H\}, \quad g \in G,$$

qui s'appellent *classes à gauche* de G *suivant* (ou *modulo*) H. On définit d'une façon analogue les *classes à droite* Hg. Chaque élément d'une classe s'appelle *représentant* de cette classe. Il est facile de voir que

$$aH = bH \Leftrightarrow a^{-1}b \in H, \tag{5}$$

$$Ha = Hb \Leftrightarrow ab^{-1} \in H. \tag{6}$$

Cela permet de définir les classes d'une autre façon. Associons à un sous-groupe H la relation $\sim$ définie dans l'ensemble G et appelée « classe à gauche suivant H » (resp. « classe à droite suivant H ») en posant par définition

$$a \sim b \Leftrightarrow a^{-1}b \in H \quad (\textit{classe à gauche})$$

(respectivement,

$$a \sim b \Leftrightarrow ab^{-1} \in H \quad (\textit{classe à droite})).$$

On vérifie sans peine que ces relations sont des relations d'équivalence sur G, i.e. qu'elles sont réflexives ($a \sim a$), symétriques ($a \sim b \Rightarrow b \sim a$) et transitives ($a \sim b$, $b \sim c \Rightarrow a \sim c$); autrement dit, elles définissent deux partitions de G en classes disjointes. En vertu de (5) et (6), ces partitions se confondent respectivement avec la partition en classes à gauche et avec la partition en classes à droite. En particulier, les classes à gauche sont disjointes deux à deux; il en est de même pour les classes à droite.

Puisque la correspondance $gH \leftrightarrow Hg^{-1}$ est bijective, le cardinal de l'ensemble des classes suivant un sous-groupe reste le même, qu'il s'agisse des classes à gauche ou à droite. Il s'appelle *indice* de sous-groupe H dans le groupe G et se note $|G : H|$.

2.4.1. Exercice. $|\mathbb{Z}:(n)| = n$.

2.4.2. Exercice. Le groupe $\mathbb{Q}$ ne contient aucun sous-groupe propre d'indice fini.

2.4.3. Exercice. $|S_n : A_n| = 2$ pour $n \geqslant 2$.

2.4.4. Exercice. Soient A, B deux sous-groupes d'un groupe G. On a alors

$$|A : A \cap B| \leqslant |G : B|. \tag{7}$$

Indication. Si les relations $\sim_1, \sim_2$ déterminent les classes à gauche de G suivant B et de A suivant $A \cap B$ respectivement, la seconde est la restriction de la première à A.

Chaque classe gH, Hg est équipotente au sous-groupe H comme le montrent les correspondances biunivoques $h \leftrightarrow gh$, $h \leftrightarrow hg$, $h \in H$. En particulier, si le groupe G est fini, on calcule son ordre $|G|$ en multipliant le cardinal $|H|$ de chaque classe par le nombre $|G : H|$ des classes. On est amené à un

2.4.5. Théorème (Lagrange). *Si H est sous-groupe d'un groupe fini G, on a*

$$|G| = |H| \cdot |G : H|. \tag{8}$$

Il donne lieu à un corollaire important: l'ordre du sous-groupe divise toujours l'ordre du groupe. Puisque $|a| = |(a)|$, l'ordre de tout élément divise aussi l'ordre du groupe.

2.4.6. Exercice. Tout groupe d'ordre fini est cyclique.

2.4.7. Exercice. Soient A, B deux sous-groupes d'un groupe G tels que $A \leqslant B$. Les indices $|G : B|$, $|B : A|$ sont tous deux finis si et seulement si l'indice $|G : A|$ est fini. Si l'indice $|G : A|$ est fini, on a

$$|G : A| = |G : B| \cdot |B : A|. \tag{9}$$

C'est une généralisation du théorème de Lagrange (lequel a lieu pour $A = 1$).

2.4.8. Exercice. L'intersection d'un nombre fini de sous-groupes d'indice fini est encore un sous-groupe d'indice fini.

Indication. A l'aide des formules (7), (9), démontrer la formule

$$|G : A \cap B| \leqslant |G : A| \cdot |G : B|. \tag{10}$$

2.4.9. Exercice. L'intersection de tous les sous-groupes d'indice fini du groupe $\mathbb{C}_p$ se confond avec le sous-groupe nul. Il en est de même pour tout autre sous-groupe propre du groupe $\mathbb{Q}$.

2.4.10. Exercice. Dans le groupe quasi cyclique $\mathbb{C}_{p^\infty}$, il n'existe aucun sous-groupe propre autre que $\mathbb{C}_{p^n}$, $n = 1, 2, \ldots$

En particulier, le groupe quasi cyclique ne contient aucun sous-groupe propre d'indice fini.

Le dernier exercice montre que les sous-groupes propres des groupes quasi cycliques sont finis, bien que les groupes eux-mêmes soient infinis. Quels sont t o u s les groupes infinis dont les sous-groupes sont finis? Ce problème posé par O. Iou. Schmidt dans les années trente s'est avéré extrêmement ardu. Il va de soi que les groupes de ce type — appelés brièvement *groupes de Schmidt* — sont nécessairement périodiques. Nous dirons qu'un groupe est *localement fini* si tous ses sous-groupes de type fini sont finis. M. I. Kargapolov a établi (*Sibirski matématitcheski journal*, 1962, **4**, n° 1, p. 232-235) que, parmi les groupes localement finis, les seuls groupes de Schmidt sont les groupes quasi cycliques. Cela explique la difficulté du problème: on est amené d'opérer dans la classe des groupes périodiques, lesquels ne sont pas localement finis, où même la recherche d'exemples isolés reste extrêmement difficile; nous en reparlerons avec plus de détails dans le § 23. Assez récemment, A. Iou. Olchanski (*Izvestia Akademii naouk SSSR*, série mathématique, 1980, **44**, n° 2, p. 309-321) a indiqué un premier exemple de groupes de Schmidt non quasi cycliques: les groupes en question sont infinis, engendrés par deux éléments, et tous leurs sous-groupes propres ont des ordres finis et même premiers.

2.5. Classes d'éléments conjugués. Un rôle particulièrement important est joué dans les groupes par les sous-groupes suivant lesquels les classes à gauche et à droite se confondent. Un tel sous-groupe est dit *normal*, ou *distingué*, ou *invariant*. Plus exactement, on dit que le sous-groupe H d'un groupe G est normal dans G (notation $H \leqslant G$) si l'on a $Hx = xH$ pour tout x appartenant à G. Si $H \leqslant G$ et $H \neq G$, on utilise la notation $H \lhd G$.

Il est clair que la condition $Hx = xH$ est équivalente à la condition $x^{-1}Hx = H$. On dit qu'un élément a est le *conjugué* d'un deuxième élément b par un troisième élément x si l'on a $a = x^{-1}bx$. On utilise souvent la notation exponentielle: $x^{-1}bx = b$. Il est facile de voir qu'on a toujours

$$(ab)^x = a^x b^x, \quad (a^x)^y = a^{xy}. \tag{11}$$

Si A, B sont deux parties d'un groupe, on a

$$A^B = \{a^b \mid a \in A,\ b \in B\}.$$

On peut dire maintenant qu'un sous-groupe H d'un groupe G est normal dans G si et seulement si, pour chacun de ses éléments, il contient aussi tous ses conjugués par des éléments appartenant à G, ou brièvement

$$H^G \subseteq H.$$

La première des formules (11) montre qu'une application du groupe G dans lui-même, telle que $a \mapsto a^x$ (pour un x donné appartenant à G) est un isomorphisme. La partie M^x est dite *conjuguée* de M dans le groupe G. D'une troisième façon, nous pouvons dire maintenant qu'un sous-groupe est normal si et seulement s'il se confond avec tous ses sous-groupes conjugués: c'est la raison pour laquelle on dit parfois autoconjugué au lieu de normal. Un groupe dont aucun sous-groupe propre n'est normal s'appelle groupe *simple*.

2.5.1. Exemples. I. II. Puisque les groupes additif et multiplicatif d'un corps commutatif sont abéliens, leur sous-groupe quelconque est normal.

III. Puisque toute permutation conjuguée d'une permutation paire est elle-même paire, on a $\mathbf{A}_n \lhd \mathbf{S}_n$.

IV. Soit $n \geqslant 2$. Puisque $\det(ab) = \det a \cdot \det b$, toute matrice de déterminant 1 admet comme conjuguée une matrice de déterminant 1, aussi $\mathbf{SL}_n(K) \trianglelefteq \mathbf{GL}_n(K)$. Puisque les éléments diagonaux se trouvant en même position dans les matrices trigonales supérieures se multiplient pendant la multiplication des matrices, on a $\mathbf{UT}_n(K) \trianglelefteq \mathbf{T}_n(K)$. En réalité, on vérifie que $\mathbf{UT}_n^m(K) \trianglelefteq \mathbf{T}_n(K)$ pour tout $m = 1, 2, \ldots$

2.5.2. Exercice. Si p est premier, $\mathbb{Z}_p$ est un groupe simple.

2.5.3. Exercice. Si $|G:H| = 2$, on a $H \lhd G$.

2.5.4. Exercice. Si $A \trianglelefteq G$, $B \trianglelefteq G$, alors $AB \trianglelefteq G$.

2.5.5. Exercice. Il peut arriver que $A \trianglelefteq B$ et $B \trianglelefteq C$ mais $A \ntrianglelefteq C$.

Soit G un groupe quelconque. Définissons une relation $\sim$ sur G en posant $a \sim b$ si a, b sont conjugués dans G. Il est facile de montrer que $\sim$ est une relation d'équivalence, i.e. qu'elle est réflexive ($a \sim a$), symétrique ($a \sim b \Rightarrow b \sim a$) et transitive ($a \sim b$, $b \sim c \Rightarrow a \sim c$). Aussi $\sim$ divise-t-elle G en *classes* disjointes *d'éléments conjugués*, ou *classes de conjugaison* a^G. En particulier, les sous-groupes normaux renfermeront chacun quelques classes de conjugaison complètes.

A la différence des classes suivant un sous-groupe, les classes d'éléments conjugués ne sont pas toujours équipotentes. Dans le calcul de leur cardinal, un rôle décisif est joué par la notion de normalisateur. Soit M une partie d'un groupe G, et soit H un sous-groupe de G. On appelle *normalisateur* de M dans H l'ensemble

$$N_H(M) = \{h \mid h \in H,\ M^h = M\},$$

qui est un sous-groupe de H, ce qui est facile à vérifier. Si l'on n'a pas indiqué le sous-groupe H, on admet que le normalisateur a été pris dans le groupe G tout entier. De toute évidence, un sous-groupe est normal dans un groupe si et seulement si son normalisateur se confond avec le groupe tout entier.

2.5.6. Théorème. *Si M est une partie du groupe G et H un sous-groupe de G, le cardinal de l'ensemble des parties conjuguées de M par des éléments de H est égal à l'indice $|H : N_H(M)|$. En particulier,*

$$|a^G| = |G : N_G(a)|.$$

Démonstration. Considérons une relation φ entre les ensembles M^x, $x \in H$, et les classes à droite de H suivant le sous-groupe $N = N_H(M)$, en posant

$$(M^x)^\varphi = Nx \text{ pour } x \in H.$$

La relation φ est univoque, car pour $M^x = M^y$ on a $Nx = Ny$. Elle associe des éléments distincts à des éléments distincts, car de $Nx = Ny$ il découle $M^x = M^y$. Enfin, φ est surjective, car tout Nx admet une image réciproque M^x. Le théorème est démontré.

2.5.7. Exemples. I. II. Puisque les groupes additif et multiplicatif d'un corps commutatif sont abéliens, leur classe de conjugaison quelconque se réduit à un élément unique.

III. Soit M un ensemble. Deux applications de $\mathbf{S}(M)$ sont conjuguées dans $\mathbf{S}(M)$ si et seulement si leurs décompositions en cycles indépendants contiennent un même nombre de cycles de chaque longueur, les cycles à un élément y compris (le nombre et la longueur sont interprétés au sens du cardinal). En effet, si

$$a = (\alpha_1\alpha_2 \ldots)(\beta_1\beta_2 \ldots)(\ldots)\ldots,$$
$$a' = (\alpha_1'\alpha_2' \ldots)(\beta_1'\beta_2' \ldots)(\ldots)\ldots,$$

les cycles de même longueur étant écrits en face, alors on vérifie immédiatement que $a' = a^x$, où

$$x = \begin{pmatrix} \alpha_1\alpha_2 & \ldots & \beta_1\beta_2 & \ldots \\ \alpha_1'\alpha_2' & \ldots & \beta_1'\beta_2' & \ldots \end{pmatrix}.$$

En particulier, deux permutations de $\mathbf{S}_n$ sont conjuguées dans $\mathbf{S}_n$ si et seulement si elles ont même structure cyclique: par exemple, la permutation (12) (3456) est la conjuguée dans $\mathbf{S}_6$ de la permutation (15) (2436) et ne l'est pas de (12) (345) (6). En ce qui concerne le groupe alterné $\mathbf{A}_n$, les éléments de même structure cyclique y forment soit une, soit deux classes de conjugaison équipotentes: cela ressort clairement du théorème 2.5.6 et de la relation $|\mathbf{S}_n : \mathbf{A}_n| = 2$.

IV. Le lecteur se rappelle que la notion de matrices conjuguées occupe une place importante dans le cours d'algèbre générale. Pour les corps commutatifs K algébriquement clos, la question de conjugaison des éléments de $\mathbf{GL}_n(K)$ est résolue complètement par le théorème de Jordan: deux matrices de $\mathbf{GL}_n(K)$ sont conjuguées dans ce groupe si et seulement si elles se laissent réduire à une même forme de Jordan.

2.5.8. Exercice. Les ordres des éléments conjugués (et, en général, les cardinaux des ensembles conjugués) sont égaux.

2.5.9. Exercice. Supposons qu'une permutation a de S_n se décompose en cycles indépendants de longueurs $n_1, \ldots, n$, $\sum n_i = n$. Calculer $|N_{S_n}(a)|$.

2.5.10. Exercice. Vérifier la formule

$$d^{-1}(\beta)\, t_{ij}(\alpha)\, d(\beta) = \begin{cases} t_{in}(\alpha\beta) & \text{pour } j = n, \\ t_{nj}\left(\frac{\alpha}{\beta}\right) & \text{pour } i = n, \\ t_{ij}(\alpha) & \text{dans les autres cas.} \end{cases}$$

A l'aide de cette formule, vérifier qu'on peut poser $r = 0$ dans l'exemple 2.2.2.IV.

2.5.11. Exercice. Les normalisateurs de tous les conjugués des éléments donnés forment une classe de conjugaison.

2.5.12. Exercice. Soit un groupe de matrices de la forme $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, $\alpha \neq 0$, sur le corps $\mathbb{Q}$. Indiquer dans ce groupe un sous-groupe conjugué de l'un de ses sous-groupes véritables.

2.5.13. Exercice. Si A est un sous-groupe d'indice fini dans un groupe G, l'intersection

$$N = \bigcap_{x \in G} A^x$$

est un sous-groupe normal d'indice fini dans G.

Indication. Utiliser le théorème 2.5.6 et l'exercice 2.4.8.

§ 3. Centre. Commutant

Nous avons vu qu'un groupe arbitraire peut différer sensiblement, d'après ses propriétés, d'un groupe de nombres. Cette différence s'explique, dans bien des cas, par la non-commutativité. Cette propriété a pour mesure le centre et le commutant: plus le centre est grand et moins le commutant est grand, plus le groupe est proche d'un groupe abélien.

3.1. Centre. Soient M une partie d'un groupe G et H un sous-groupe de G. Nous avons appelé normalisateur de M dans H l'ensemble des éléments de H qui commutent avec M tout entier. On peut aussi considérer l'ensemble des éléments de H qui commutent avec M élément par élément, i.e.

$$C_H(M) = \{x \mid x \in H,\ \ m^x = m \text{ pour tout } m \in M\}.$$

Cet ensemble s'appelle le *centralisateur* de M dans H; on voit sans peine que c'est un sous-groupe normal du normalisateur $N_H(M)$.

Si M se réduit à un élément unique, il va de soi que son normalisateur et son centralisateur dans H se confondent. Si le sous-groupe H n'est pas indiqué, on admet que le centralisateur est pris dans G tout entier.

Le centralisateur du groupe G tout entier s'appelle *centre* et se note $Z(G)$. De toute évidence, un groupe est abélien si et seulement s'il se confond avec son centre. Il est clair que l'unité est toujours contenue dans le centre. Si le groupe ne contient aucun élément central sauf l'unité, il s'appelle *groupe de centre trivial* et même *groupe sans centre*. Remarquons en outre que tout sous-groupe du centre est normal dans le groupe.

A titre d'illustration, définissons les centres dans les groupes I à IV du § 1.

3.1.1. Exemples. I. II. Puisque les groupes additif et multiplicatif d'un corps commutatif sont abéliens, ils se confondent avec leur centre.

III. Il est évident que les groupes $\mathbf{S}_2$ et $\mathbf{A}_3$ sont abéliens et se confondent donc avec leur centre. Ensuite, toute permutation non identique dans $\mathbf{S}_n$, décomposée en cycles indépendants se présente sous la forme $(ij\ldots)(\ldots)\ldots$ On vérifie immédiatement qu'elle ne commute pas avec la transposition (jk) pour $n \geqslant 3$, ni avec le cycle à trois éléments (jkl) pour $n \geqslant 4$ (les lettres différentes désignent des symboles différents). Cela veut dire que les groupes $\mathbf{S}_n$ et $\mathbf{A}_n$ admettent un centre trivial pour $n \geqslant 3$ et $n \geqslant 4$ respectivement.

IV. Soit K un corps commutatif. Les centres des groupes $\mathbf{GL}_n(K)$, $\mathbf{SL}_n(K)$ sont formés par des matrices scalaires contenues dans ces groupes. En effet, toute matrice scalaire est évidemment contenue dans le centre. Réciproquement, si a est un élément central de $\mathbf{GL}_n(K)$ ou de $\mathbf{SL}_n(K)$, il commute avec toutes les transvections $t_{ij} = t_{ij}(1)$, i.e. $at_{ij} = t_{ij}a$. D'où l'on déduit sans peine que

$$a_{ij} = 0, \quad a_{ii} = a_{jj} \text{ pour tout } i \neq j,$$

i.e. a est une matrice scalaire. Dans les calculs analogues à celui-ci, nous conseillons au lecteur d'écrire chaque matrice x sous la forme $\sum x_{rs}e_{rs}$ et d'employer la table de multiplication connue des unités matricielles:

$$e_{ij}e_{rs} = \begin{cases} e_{is} & \text{pour } j = r, \\ 0 & \text{pour } j \neq r. \end{cases} \tag{1}$$

Des raisonnements analogues montrent que le centre du groupe $\mathbf{T}_n(K)$, $|K| \neq 2$, est formé par toutes les matrices scalaires non nulles et que les matrices centrales du groupe $\mathbf{UT}_n^m(K)$ sont exactement celles qui ne diffèrent de la matrice e que par le bloc supérieur de droite d'ordre m. En particulier,

$$Z(\mathbf{UT}_n(K)) = \mathbf{UT}_n^{n-1}(K) = \{t_{1n}(\alpha) \mid \alpha \in K\}. \tag{2}$$

Le groupe $\mathbf{D}_n(K)$ est abélien et se confond donc avec son centre.

3.1.2. Exercice. Chercher le centralisateur d'une matrice diagonale dans $\mathbf{GL}_n(K)$.

3.1.3. Exercice. Le centralisateur d'un sous-groupe normal est encore un sous-groupe normal.

3.1.4. Exercice. Si H est un sous-groupe normal fini d'un groupe G, son centralisateur est d'indice fini.

Solution:

$$|G : C_G(H)| = |G : \bigcap_{x \in H} C_G(x)| \leqslant \prod_{x \in H} |G : C_G(x)| \leqslant |H|^{|H|}.$$

3.1.5. Exercice. Le groupe de matrices $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, $\alpha \neq 0$, sur un corps commutatif autre que $\mathbf{GF}(2)$ a un centre trivial.

3.1.6. Exercice. $|Z(\mathbf{GL}_n(q))| = q - 1$, $|Z(\mathbf{SL}_n(q))| = \operatorname{pgcd}(n, q-1)$.

3.1.7. Exercice. Le centre d'un produit direct (cartésien) se confond avec le produit direct (cartésien) des centres des facteurs.

3.2. Commutant. Il est évident que deux éléments a, b d'un groupe G commutent si et seulement si $a^{-1}b^{-1}ab = e$. Le premier membre de cette relation s'appelle *commutateur* des éléments a, b (pris dans cet ordre) et se note $[a, b]$. Le sous-groupe engendré dans G par tous les commutateurs s'appelle le *commutant* de G. Il est clair qu'un groupe est commutatif si et seulement si son commutant est égal à l'unité; en général, le commutant est pour ainsi dire la mesure de la non-commutativité.

D'une façon plus générale, étant données deux parties L, M d'un groupe G, leur *commutant réciproque* est le sous-groupe

$$[L, M] = \operatorname{gr}([a, b] \mid a \in L,\ b \in M).$$

Puisque

$$[a, b]^x = [a^x, b^x],$$

le commutant réciproque de deux sous-groupes normaux est lui-même un sous-groupe normal. En particulier, le commutant $[G, G]$ du groupe G est un sous-groupe normal. Prenant le commutant d'un commutant et ainsi de suite, nous obtenons une suite décroissante de sous-groupes normaux

$$G \geqslant G' \geqslant G'' \ldots$$

appelée *série de commutants* du groupe G. Le commutant est parfois appelé *groupe dérivé*, et la série de commutants, *série dérivée*.

Voici quelques relations utiles entre commutateurs, qui se laissent vérifier immédiatement:

$$[a, b]^{-1} = [b, a],\ [ab, c] = [a, c]^b [b, c],\ [a^{-1}, b] = [b, a]^{a^{-1}}. \quad (3)$$

Reprenons comme précédemment les groupes I à IV du § 1 afin d'illustrer la notion introduite.

3.2.1. Exemples. I. II. Puisque les groupes additif et multiplicatif d'un corps commutatif sont abéliens, leurs commutants sont égaux à l'unité.

III. Il est évident que $[S_2, S_2] = 1$, $[A_3, A_3] = 1$. Ensuite

$$[A_4, A_4] = \{1, (12)(34), (13)(24), (14)(23)\}. \tag{4}$$

En effet, on vérifie immédiatement que le second membre est un sous-groupe (appelé *Vierergruppe* ou *4-groupe de Klein*). C'est même un sous-groupe normal dans A_4, car il contient toutes les permutations du type (**) (**); or, nous savons que le type cyclique d'une permutation reste inchangé par toute conjugaison. Puisque A_n est engendré par les différents cycles à trois éléments, pour qu'il y ait inclusion $\subseteq$, il suffit, compte tenu des formules (3) et de la normalité du second membre de (4), que les commutateurs produits par les cycles à trois éléments soient inclus au second membre. Or, cela ressort immédiatement des relations

$$[(ijk), (ijl)] = (ij)(kl), \quad [(ijk), (ilj)] = (il)(jk)$$

immédiates elles aussi (les lettres différentes désignent des symboles différents). Les mêmes relations prouvent qu'il y a aussi inclusion réciproque. Enfin,

$$[S_n, S_n] = A_n \text{ pour tout } n, \tag{5}$$

$$[A_n, A_n] = A_n \text{ pour } n \geqslant 5. \tag{6}$$

En effet, le commutateur de deux permutations quelconques de S_n est une permutation paire et appartient donc à A_n. D'autre part,

$$(ijk) = [(ik), (ij)] = [(ikl), (ijm)]$$

(les lettres différentes désignent des symboles différents). Puisque A_n est engendré par des cycles à trois éléments, notre assertion est démontrée.

IV. Soit K un corps commutatif. On a toujours

$$[GL_n(K), GL_n(K)] = SL_n(K), \tag{7}$$

$$[SL_n(K), SL_n(K)] = SL_n(K), \tag{8}$$

à l'exception du groupe $GL_2(2)$ dans (7) et des groupes $SL_2(2)$, $SL_2(3)$ dans (8) (remarquons d'ailleurs que $GL_2(2) = SL_2(2)$, si bien qu'on n'a que deux exceptions). En effet, le déterminant du commutateur de deux matrices quelconques est égal à 1, aussi les inclusions $\subseteq$ sont-elles évidentes. D'autre part, nous savons

que $SL_n(K)$ est engendré par des transvections. Il est facile de voir que

$$[t_{ik}(\alpha),\ t_{kj}(\beta)] = t_{ij}(\alpha\beta) \text{ pour } i,\ j,\ k \text{ différents}, \tag{9}$$

$$[t_{ij}(\alpha),\ \operatorname{diag}(\beta_1, \ldots, \beta_n)] = t_{ij}\left(\alpha\left(\frac{\beta_j}{\beta_i} - 1\right)\right). \tag{10}$$

En vertu de (9), on a aussi les inclusions réciproques pour $n \geqslant 3$. Soit maintenant $n = 2$. Puisque pour $|K| > 2$ on peut choisir $\beta_1 \neq \beta_2$ dans (10), la formule (7) a lieu pour tous les groupes sauf pour $GL_2(2)$. Puisque pour $|K| > 3$ on peut choisir $\beta_1 \neq \beta_2$, $\beta_1\beta_2 = 1$, la formule (8) a lieu pour tous les groupes sauf pour $SL_2(2)$, $SL_2(3)$. Les groupes indiqués doivent vraiment être exceptés: on montre qu'ils ne vérifient pas les formules (7), (8).

D'une façon analogue, utilisant les formules (3), (4) du paragraphe précédent et les formules (9), (10), nous montrerons que

$$[T_n(K),\ T_n(K)] = UT_n(K) \text{ pour } |K| > 2, \tag{11}$$

$$[UT_n^r(K),\ UT_n^r(K)] = UT_n^{r+}(K). \tag{12}$$

Pour $|K| = 2$, la formule (11) cesse d'être vraie, mais on a dans ce cas $T_n(K) = UT_n(K)$, si bien que la formule (12) reste applicable.

3.2.2. Lemme. *Soient G un groupe quelconque, A, B ses deux sous-groupes, $H = \operatorname{gr}(A, B)$. Alors*

$$[A, B],\ A[A, B],\ B[A, B] \textit{ sont normaux dans } H, \tag{13}$$

$$A[A, B] \cdot B[A, B] = H \tag{14}$$

$$[A, B] = \operatorname{gr}(\operatorname{gr}(C^A))^B, \tag{15}$$

où $C = \{[a_i, b_j] \mid i \in I,\ j \in J\}$ *si* $A = \operatorname{gr}(a^i \mid i \in I)$, $B = \operatorname{gr}(b_j \mid j \in J)$.

Démonstration. La seconde des identités (3) montre que le sous-groupe A normalise $[A, B]$; il s'ensuit que les conclusions (13) et (14) deviennent alors évidentes. Démontrons (15). Puisque $C \subseteq [A, B] \trianglelefteq H$, on a évidemment $D \leqslant [A, B]$, où D désigne le second membre de (15). Vérifions maintenant que $[A, B] \leqslant D$. Il s'agit de montrer que

$$[a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m},\ b_{j_1}^{\delta_1} \ldots b_{j_n}^{\delta_n}] \in D \text{ pour } \varepsilon_i = \pm 1,\ \delta_j = \pm 1.$$

Il vient

$$(a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m})^{b_j} = (a_{i_1}[a_{i_1}, b_j])^{\varepsilon_1} \ldots (a_{i_m}[a_{i_m}, b_j])^{\varepsilon_m} =$$
$$= a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m} f,\quad f \in \operatorname{gr}(C^A),$$

i.e.

$$[a, b_j] \in \mathrm{gr}(C^A), \quad \text{où} \quad a = a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m}.$$

D'où

$$(b_{j_1}^{\delta_1} \ldots b_{j_n}^{\delta_n})^a = (b_{j_1}[b_{j_1}, a])^{\delta_1} \ldots (b_{j_n}[b_{j_n}, a])^{\delta_n} =$$
$$= b_{j_1}^{\delta_1} \ldots b_{j_n}^{\delta_n} d, \quad d \in D,$$

ce qu'il fallait démontrer.

Soient maintenant $a_1, a_2, \ldots$ et $A_1, A_2, \ldots$ respectivement éléments et sous-groupes d'un groupe. Posons par récurrence

$$[a_1, \ldots, a_{n+1}] = [[a_1, \ldots, a_n], a_{n+1}],$$
$$[A_1, \ldots, A_{n+1}] = [[A_1, \ldots, A_n], A_{n+1}]$$

pour $n \geqslant 2$.

3.2.3. Lemme des trois commutants. *Soient A, B, C trois sous-groupes d'un groupe et H un sous-groupe normal de ce dernier. Si deux quelconques des commutants*

$$[A, B, C], [B, C, A], [C, A, B]$$

sont contenus dans H, il en est de même du troisième.

Démonstration. Elle découle de la relation élégante qui se vérifie immédiatement (identité de Ph. Hall):

$$[a, b^{-1}, c]^b [b, c^{-1}, a]^c [c, a^{-1}, b]^a = 1. \tag{10}$$

3.2.4. Exercice. Chercher les séries dérivées dans les groupes S_3, S_4.

3.2.5. Exercice. Chercher les commutants dans les groupes $SL_2(2)$, $SL_2(3)$.

3.2.6. Exercice. Si A, B, C sont trois sous-groupes normaux d'un groupe, on a $[AB, C] = [A, C]\cdot[B, C]$.

3.2.7. Exercice. Le commutant d'un produit direct de groupes est le produit direct des commutants des facteurs. Peut-on mettre « cartésien » au lieu de « direct »?

3.2.8. Exercice. Chercher le commutant du groupe de matrices $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, $\alpha \neq 0$ sur un corps commutatif et montrer que chaque élément de ce commutant est un commutateur.

Nous attirons l'attention du lecteur sur le fait que le commutant d'un groupe ne se réduit généralement pas à des commutateurs. Il existe même des groupes finis où le produit de deux commutateurs n'est égal à aucun commutateur. Avant de terminer ce paragraphe,

nous donnerons un exemple de groupe de ce type avec une esquisse de la démonstration :

3.2.9. Exemple. Définissons un ensemble S de dix symboles régi par la table de multiplication suivante :

$\cdot$	1	α	β	γ	δ	$\varkappa$	λ	μ	ν	0
1	1	α	β	γ	δ	$\varkappa$	λ	μ	ν	0
α	α	0	$\varkappa$	λ	μ	0	0	0	0	0
β	β	0	0	ν	0	0	0	0	0	0
γ	γ	0	0	0	0	0	0	0	0	0
δ	δ	0	0	0	0	0	0	0	0	0
$\varkappa$	$\varkappa$	0	0	0	0	0	0	0	0	0
λ	λ	0	0	0	0	0	0	0	0	0
μ	μ	0	0	0	0	0	0	0	0	0
ν	ν	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0

On voit sans peine que la multiplication dans S est associative : on dit alors que S est un *demi-groupe*. Soit K un anneau de demi-groupes pour S, sur le corps **GF** (2), i.e. l'anneau des combinaisons formelles

$$n_1 1 + n_2\alpha + n_3\beta + n_4\gamma + n_5\delta + n_6\varkappa + n_7\lambda + n_8\mu + n_9\nu + n_{10}0$$

à coefficients dans **GF** (2), par rapport aux opérations d'addition et de multiplication naturelles. Soit enfin G l'ensemble des matrices sur K de la forme

$$a = \begin{pmatrix} 1 & x & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$

On vérifie facilement que G est un groupe d'ordre 2^{20} et que si

$$b = \begin{pmatrix} 1 & u & v \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix}, \text{ alors } [a, b] = \begin{pmatrix} 1 & 0 & xu - ux \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (17)$$

Nous dirons que $xu - ux$ est le commutateur annulaire de x et u.

3.2.10. Exercice. L'élément $\mu + \nu$ est une somme de deux commutateurs annulaires sans être un commutateur annulaire lui-même.

3.2.11. Exercice. Compte tenu de (17), continuer l'exercice précédent et indiquer dans G un produit de deux commutateurs qui n'est plus un commutateur.

CHAPITRE 2

HOMOMORPHISMES

§ 4. Homomorphismes et groupes quotients

4.1. Définitions. D'après une des définitions initiales, l'application d'un groupe dans un autre est un isomorphisme si elle est biunivoque et si elle conserve l'opération. Abandonnant la première exigence, on aboutit à la notion d'homomorphisme : l'application φ du groupe G dans le groupe G^* est appelée *homomorphe*, ou *homomorphisme*, si $(ab)^\varphi = a^\varphi b^\varphi$ pour deux éléments quelconques a, b de G.

4.1.1. Exemples. I. L'application $\mathbb{Z} \to \mathbb{Z}_n$ qui fait correspondre à un entier relatif son résidu modulo n est une application homomorphe. Soient p un nombre premier et ε_n une racine primitive p^n-ième de 1 sur le corps des nombres complexes, et soient $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1, 2, \ldots$ L'application $\mathbb{Q}_p \to \mathbb{C}_{p\infty}$ qui fait correspondre à une fraction p-aire m/p^n un nombre complexe ε_n^m est bien déterminée et est un homomorphisme.

II. L'application $\mathbb{R}^* \to \mathbb{Z}^*$ qui fait correspondre à chaque nombre dans $\mathbb{R}^*$ son signe est un homomorphisme.

III. L'application $\mathbf{S}_n \to \mathbb{Z}^*$ qui fait correspondre à chaque permutation son signe en fonction de sa parité est un homomorphisme.

IV. Quelques autres exemples d'homomorphismes : l'application $\mathbf{GL}_n(K) \to K^*$ qui fait correspondre à une matrice son déterminant ; l'application $\mathbf{T}_n(K) \to \mathbf{D}_n(K)$ qui fait correspondre à une matrice trigonale sa diagonale ; l'application $\mathbf{UT}_n^m(K) \to K \oplus \ldots \oplus K$ ($n - m$ fois) qui fait correspondre à une matrice x la ligne $\langle x_{1,\, m+1}, x_{2,\, m+2}, \ldots, x_{n-m,\, m}\rangle$.

Nous voyons que certaines propriétés de l'opération algébrique risquent de disparaître dans une application homomorphe : un groupe non commutatif peut devenir commutatif, un groupe apériodique peut devenir périodique et ainsi de suite ; d'autre part, les traits les plus remarquables, tels que la finitude, la commutativité, etc. restent inchangés par tout homomorphisme. On peut dire que toute image homomorphe d'un groupe G est un vague souvenir, où seuls restent les traits les plus marquants de G au point de vue de l'homomorphisme « témoin oculaire ». Pauvre en détails, il caractérise mal le personnage ; or, il n'en est que plus facile à étudier. En outre, il

suffit d'interroger plusieurs témoins oculaires pour rassembler toute l'information nécessaire sur G. Par exemple, sachant que les groupes $\mathbb{Z}_2$, $\mathbb{Z}_3$, ... sont des images homomorphes du groupe G, on peut affirmer que G est un groupe infini, bien que la connaissance de chaque image isolée ne permette pas de conclure à l'infinitude.

4.1.2. Exercice. L'image homomorphe d'un sous-groupe (normal) est un sous-groupe (normal). La restriction d'un homomorphisme à un sous-groupe est un homomorphisme du sous-groupe.

Soit φ un homomorphisme d'un groupe G dans un groupe G^*. L'ensemble des éléments de G dont l'image par φ est l'unité s'appelle *noyau* de l'homomorphisme φ et se note Ker φ. Le noyau de tout homomorphisme est un sous-groupe normal. Soit en effet Ker $\varphi = H$. Puisque

$$(HH)^\varphi = H^\varphi H^\varphi = 1, \quad (H^{-1})^\varphi = (H^\varphi)^{-1} = 1,$$
$$(H^G)^\varphi = (H^\varphi)^{G^\varphi} = 1,$$

on a

$$HH \subseteq H, \quad H^{-1} \subseteq H, \quad H^G \subseteq H$$

Or, cela revient à dire précisément que $H \trianglelefteq G$. Ensuite, on comprend facilement que le noyau de l'homomorphisme φ est trivial (Ker $\varphi = 1$) si et seulement si φ est un isomorphisme. Dans le cas général, on peut dire que le noyau de l'homomorphisme est inversement proportionnel à la force de sa mémoire : plus le noyau est vaste, moins l'homomorphisme a de mémoire. Un homomorphisme qui n'a pratiquement plus de mémoire se rappelle seulement que le groupe avait une unité.

Il se trouve que les sous-groupes normaux du groupe sont les seuls noyaux d'homomorphismes, i.e. que chaque sous-groupe normal est noyau d'un homomorphisme. Il existe un procédé canonique de recherche d'un homomorphisme d'après son noyau. Soient G un groupe, H son sous-groupe normal, G/H l'ensemble des classes de G suivant H (il ne sert à rien de préciser si la classe est à gauche ou à droite : elles se confondent toutes, car H est normal). On voit sans peine que $aH \cdot bH = abH$, i.e. que l'ensemble G/H est fermé par rapport à la multiplication des classes élément par élément. On vérifie sans difficulté en outre que G/H est un groupe par rapport à cette multiplication ; il porte le nom de *groupe quotient* du groupe G par son sous-groupe normal H. L'unité dans le groupe G/H est la classe H ; l'inverse de la classe aH est la classe $a^{-1}H$. Soulignons que la classe aH est une classe d'éléments dans le groupe G, tandis que dans le groupe G/H elle n'est pas une classe mais un élément. On voit immédiatement que la surjection φ: $G \to G/H$ régie par la loi $g^\varphi = gH$ est un homomorphisme. De tels homomorphismes sont dits

naturels ou canoniques. Ils résolvent notre problème: c'est H qui constitue le noyau de l'homomorphisme naturel $G \to G/H$.

4.1.3. Exercice. Un groupe quotient d'un groupe cyclique est un groupe cyclique.

4.1.4. Exercice. Le groupe quotient G/H est abélien si et seulement si H contient le commutant $[G, G]$.

Une autre approche de la notion de groupe quotient, différente de celle qui précède, donne lieu à un

4.1.5. Exercice. Une relation d'équivalence $\sim$ introduite dans un groupe est appelée *congruence* si l'on a toujours

$$a \sim b,\ a' \sim b' \Rightarrow aa' \sim bb'.$$

Le produit de deux classes de congruence est encore une classe de congruence. L'ensemble $G/\sim$ de toutes les classes de congruence est un groupe par rapport à la multiplication des classes. Il s'appelle *groupe quotient* du groupe G par la congruence $\sim$. Une notion analogue s'obtient sans peine pour un système quelconque muni d'opérations.

4.1.6. Exercice. Toutes les congruences dans un groupe sont en correspondance biunivoque avec les sous-groupes normaux de G. En effet, si $H \leqslant G$ et si l'on a par définition

$$a \sim b \Leftrightarrow a^{-1}b \in H,$$

la relation $\sim$ est une congruence et les classes de G suivant H sont des classes de congruence. Réciproquement, étant donnée une congruence $\sim$ dans G, l'ensemble H des éléments congrus à l'unité est un sous-groupe normal dans G et les classes de congruence sont des classes de G suivant H. Les groupes quotients par les congruences se confondent donc avec les groupes quotients par les sous-groupes normaux. Dans d'autres systèmes munis d'opérations, la notion de système quotient par les congruences a lieu comme précédemment, bien qu'on n'y trouve parfois rien qui ressemble à un sous-groupe normal. Ainsi donc, l'approche définie dans l'exercice 4.1.5 est équivalente à la précédente quand on examine des groupes; dans une situation plus générale, c'est la première approche qui est la meilleure.

4.1.7. Théorème. (Passage au quotient. Rang.) *Si H est un sous-groupe normal d'un groupe G, on a*

$$\operatorname{rang} G \leqslant \operatorname{rang} H + \operatorname{rang} G/H.$$

Démonstration. Soient r, s les rangs des groupes H et G/H respectivement. Choisissons une partie finie M de G et considérons dans le groupe quotient G/H le sous-groupe engendré par les

éléments xH, $x \in M$. Comme il s'agit d'un groupe de type fini, on peut choisir dans gr (M) une partie S de cardinal s, telle que

$$\mathrm{gr}\,(xH \mid x \in \mathrm{M}) = \mathrm{gr}\,(xH \mid x \in S).$$

Attribuons une notation déterminée à chaque $x \in M$:

$$x = x_S x_H, \quad x_S \in \mathrm{gr}\,(S), \quad x_H \in H.$$

Puisque gr $(x_H \mid x \in M)$ est un sous-groupe de type fini dans H, il est engendré par une partie R de cardinal $\leqslant r$. On voit maintenant que gr $(M) = \mathrm{gr}\,(R \cup S)$, i.e. que rang $G \leqslant r + s$.

4.2. Théorèmes des homomorphismes. Soient G un groupe, H un sous-groupe de G. Désignons par $L\,(G, H)$ l'ensemble des sous-groupes de G qui contiennent H. En particulier, $L\,(G, 1)$ est l'ensemble des sous-groupes de G. On a un théorème sur la correspondance des sous-groupes par un homomorphisme.

4.2.1. Théorème. *Etant donné un homomorphisme canonique $\varphi: G \to G/H$, il existe une application $\psi: L\,(G, H) \to L\,(G/H, 1)$ qui fait correspondre aux sous-groupes dans $L\,(G, H)$ leurs images par φ. Cette ψ est une bijection. Deux sous-groupes A, B de $L\,(G, H)$ sont conjugués dans G si et seulement si leurs images A^ψ, B^ψ le sont dans G/H. En particulier, A est un sous-groupe normal dans G si et seulement si A^ψ l'est dans G/H. Si $A \leqslant B$, on a $|B : A| = |B^\psi : A^\psi|$.*

Démonstration. L'application ψ fait correspondre aux sous-groupes différents A, B de $L\,(G, H)$ des sous-groupes différents: si $a \in A$, $a \notin B$, on a $a^\varphi \in A^\varphi$, $a^\varphi \notin B^\varphi$. En effet, si $a^\varphi \in B^\varphi$, on aurait $a^\varphi = b^\varphi$, $b \in B$, d'où $b^{-1}a \in H \leqslant B$, $a \in B$ contrairement à l'hypothèse. Ensuite, ψ est une surjection, car l'image réciproque d'un sous-groupe donné $\bar{A}$ de G/H par ψ est l'image réciproque de $\bar{A}$ par φ. On vérifie tout aussi aisément que

$$B = A^x \Leftrightarrow B^\varphi = (A^\varphi)^{x^\varphi}.$$

Enfin, si $A \leqslant B$, il existe une correspondance biunivoque entre les classes à gauche de B suivant A et les classes à gauche de B^ψ suivant A^ψ, car

$$x^{-1}y \in A \Leftrightarrow (xH)^{-1}\,(yH) \in A/H.$$

Le théorème est démontré.

Il se trouve que les homomorphismes d'un groupe se réduisent pratiquement tous à des homomorphismes naturels; plus exactement, tout homomorphisme s'obtient en opérant un homomorphisme canonique suivi d'un isomorphisme. Nous allons voir que les « homo-

morphismes ayant même noyau se rappellent, tous, les mêmes traits du groupe : leurs souvenirs sont isomorphes ».

4.2.2. Théorème. *Si φ est un homomorphisme d'un groupe G de noyau H, on a $G^\varphi \simeq G/H$. Bien plus, l'homomorphisme φ revient à opérer d'abord l'homomorphisme canonique ε : $G \to G/H$ et puis un isomorphisme τ : $G/H \to G^\varphi$.*

Démonstration. Caractérisons l'application τ: $G/H \to G^\varphi$ en posant

$$(xH)^\tau = x^\varphi \text{ pour } x \in G.$$

C'est bien une application, car de $xH = yH$ il ressort que $x^\varphi = y^\varphi$. L'application τ fait correspondre aux éléments différents des éléments différents, car $x^\varphi = y^\varphi$ implique $x^{-1}y \in H$. Ensuite, τ est une surjection, ce qui est évident. Enfin, τ conserve la multiplication, car

$$(xH \cdot yH)^\tau = (xyH)^\tau = (xy)^\varphi = x^\varphi y^\varphi = (xH)^\tau (yH)^\tau.$$

Donc τ est un isomorphisme de G/H sur G^φ. Il est clair maintenant que $\varphi = \varepsilon\tau$. Le théorème est démontré.

A titre d'illustration, appliquons ce théorème aux exemples 4.1.1. Calculant les noyaux des homomorphismes signalés, on obtient les formules suivantes :

$$\mathbb{Z}/(n) \simeq \mathbb{Z}_n, \tag{1}$$

$$\mathbb{Q}_p/\mathbb{Z} \simeq \mathbb{C}_{p^\infty}, \tag{2}$$

$$\mathbf{S}_p/\mathbf{A}_n \simeq \mathbb{Z}^* \simeq \mathbb{Z}_2, \tag{3}$$

$$\mathbf{GL}_n(K)/\mathbf{SL}_n(K) \simeq K^*, \tag{4}$$

$$\mathbf{T}_n(K)/\mathbf{UT}_n(K) \simeq \mathbf{D}_n(K) \simeq \underbrace{K^* \times \ldots \times K^*}_{n \text{ fois}}, \tag{5}$$

$$\mathbf{UT}_n^m(K)/\mathbf{UT}_n^{m+1}(K) \simeq \underbrace{K \oplus \ldots \oplus K}_{n-m \text{ fois}}. \tag{6}$$

Au moyen du théorème 4.2.2, poursuivons l'étude de l'application ψ: $L(G, H) \to L(G/H, 1)$ définie dans le théorème 4.2.1 et montrons que les sous-groupes normaux correspondants définissent des groupes quotients isomorphes.

4.2.3. Théorème. *Si $H \trianglelefteq G$, $A \trianglelefteq G$ et $H \leqslant A$, on a*

$$(G/H)/(A/H) \simeq G/A.$$

Démonstration. Etablissons la relation φ: $G/H \to G/A$ en posant

$$(xH)^\varphi = xA \text{ pour } x \in G.$$

C'est une application, car de $xH = yH$ il ressort que $x^{-1}y \in H \leqslant A$, $xA = yA$. Ensuite, φ est une surjection, ce qui est évident. Enfin, φ conserve la multiplication, car

$$(xH \cdot yH)^{\varphi} = (xyH)^{\varphi} = xyA = xA \cdot yA.$$

Ainsi donc, φ est un homomorphisme de G/H sur G/A. On a évidemment $\operatorname{Ker} \varphi = A/H$, donc $A/H \trianglelefteq G/H$, tandis que l'isomorphisme résulte du théorème 4.2.2.

4.2.4. Théorème. *Si $A \trianglelefteq B \leqslant G$ et $H \trianglelefteq G$, on a*

$$BH/AH \simeq B/A\,(B \cap H).$$

En particulier,

$$BH/H \simeq B/B \cap H.$$

Démonstration. Il est évident que $AH \trianglelefteq BH$ et que la restriction au sous-groupe B de l'homomorphisme naturel $BH \to BH/AH$ admet comme noyau $B \cap AH$ et comme image BH/AH. Appliquant le théorème 4.2.2 à cette restriction, on obtient $BH/AH \simeq B/B \cap AH$. Il ne reste qu'à faire intervenir l'égalité évidente $B \cap AH = A\,(B \cap H)$. Le théorème est démontré.

4.2.5. Exercice. Si $G = A \times B$, on a $G/A \simeq B$.

4.2.6. Exercice. Soit H un sous-groupe de $\mathbb{C}^*$ composé de tous les nombres complexes de module 1 ; soit $\mathbb{R}^{**}$ le groupe multiplicatif des nombres réels strictement positifs. On a alors $\mathbb{C}^*/H \simeq \mathbb{R}^{**}$.

Le lecteur connaît sûrement, du cours d'algèbre générale, ce que sont un groupe, un sous-groupe, un sous-groupe normal, un homomorphisme, un groupe quotient ; nous croyons cependant utile, dans un livre intitulé *Eléments de la théorie des groupes*, de faire un bref rappel des notions connues. Il est probablement superflu de rappeler des notions analogues telles qu'un sous-anneau, un idéal, un homomorphisme d'anneaux et un anneau quotient. Un lien fort intéressant apparaît entre les premières et les secondes notions quand on étudie les groupes de matrices sur les anneaux.

4.2.7. Exercice. Soit K un anneau associatif unitaire, et soit G un groupe de matrices d'ordre n sur K. Si $\mathfrak{a}$ est un idéal dans K, alors

$$G_{\mathfrak{a}} = \{e + a \mid e + a \in G,\ \ a_{ij} \in \mathfrak{a}\}$$

est un sous-groupe normal dans G. Il s'appelle *sous-groupe de congruence principal* modulo $\mathfrak{a}$, et ses surgroupes sont appelés *sous-*

groupes de congruence de G. Tout homomorphisme d'anneaux $\varphi : K \to K'$ induit un homomorphisme de groupes $\varphi_G : G \to G'$ régi par la loi

$$(g_{ij})^{\varphi_G} = (g_{ij}^{\varphi}), \quad g \in G.$$

Son noyau est $\operatorname{Ker} \varphi_G = G_{\operatorname{Ker}\varphi}$. Par exemple, l'homomorphisme $\mathbb{Z} \to \mathbb{Z}_m$ induit l'homomorphisme $\mathbf{SL}_n(\mathbb{Z}) \to \mathbf{SL}_n(\mathbb{Z}_m)$ dont le noyau (le m-ième sous-groupe de congruence principal) se note $\Gamma_n(m)$. Chaque $\Gamma_n(m)$ est d'indice fini dans $\mathbf{SL}_n(\mathbb{Z})$. En général, l'homomorphisme d'anneaux $K \to K/\mathfrak{a}$ induit des homomorphismes de groupes $\mathbf{GL}_n(K) \to \mathbf{GL}_n(K/\mathfrak{a})$, $\mathbf{SL}_n(K) \to \mathbf{SL}_n(K/\mathfrak{a})$, etc.; leurs noyaux — les sous-groupes de congruence principaux modulo $\mathfrak{a}$ — se notent respectivement $\mathbf{GL}_n(K, \mathfrak{a})$, $\mathbf{SL}_n(K, \mathfrak{a})$, etc. En particulier, $\Gamma_n(m) = \mathbf{SL}_n(\mathbb{Z}, m\mathbb{Z})$.

En liaison avec le dernier exercice, on voit se poser un très important *problème de congruence* pour le groupe matriciel G: tout sous-groupe d'indice fini dans G contient-il G_I suivant un idéal I d'indice fini? Nous citerons en page 185 un des tous premiers exemples de solution positive du problème de congruence. Notons que J. L. Mennicke (*Ann. Math.*, 1965, **81**, n° 1, p. 31-37) et indépendamment H. Bass, M. Lazard et J.-P. Serre (*Bull. Amer. Math. Soc.*, 1964, **70**, n° 3, p. 385-392) ont trouvé une solution positive du problème de congruence pour le groupe $\mathbf{SL}_n(\mathbb{Z})$, $n \geqslant 3$ (pour $n = 2$ la solution négative était connue depuis longtemps). Le travail de Mennicke est accessible à un étudiant de deuxième année.

4.2.8. Exercice. Soient p un nombre premier, m, n deux entiers naturels, $m \geqslant 2$. Considérons dans $\mathbf{GL}_n(\mathbb{Z}_{p^m})$ les sous-groupes de congruence principaux

$$P_k = \mathbf{GL}_n(\mathbb{Z}_{p^m}, p^k\mathbb{Z}_{p^m}),$$

i.e.

$$P_k = \{e + p^k a \mid a \in \mathbf{M}_n(\mathbb{Z}_{p^m})\}, \quad k = 1, 2, \ldots$$

On demande de montrer que l'application $\varphi_k : P_k \to P_{m-1}$ régie par la loi

$$e + p^k a \mapsto e + p^{m-1}a, \qquad a \in \mathbf{M}_n(\mathbb{Z}_{p^m}),$$

est un homomorphisme *surjectif* (épimorphisme) de noyau P_{k+1}. Cet homomorphisme se confond avec l'élévation des matrices à la puissance p^{m-k-1}, à l'exception du cas où $p = 2$ et $k = 1$.

4.3. Produits sous-cartésiens. Rappelons que le produit direct

$$G = \prod_{i \in I} G_i \tag{7}$$

est composé de fonctions $f: I \to \bigcup_{i \in I} G_i$ telles que

1° $f(i) \in G_i$ pour tout $i \in I$,
2° $|\operatorname{supp}(f)| < \infty$.

On vérifie sans difficulté que la partie

$$G'_i = \{f \mid f \in G,\ f(j) = e \text{ pour } j \neq i\}$$

est un sous-groupe normal dans G, qui est isomorphe au facteur G_i, car $f \to f(i)$. En vertu de cet isomorphisme, G'_i est souvent identifié à G_i, auquel cas on a $G_i \trianglelefteq G$, le groupe G est engendré par les sous-groupes G_i et chaque élément g de G peut s'écrire sous la forme

$$g = g_{i_1} \ldots g_{i_m},\ g_i \in G_i, \tag{8}$$

où tous les symboles $i_1, \ldots, i_m$ sont distincts et les facteurs différents de l'unité se déterminent d'une façon unique par l'élément g.

Cette remarque permet de donner une définition intérieure du produit direct, à la différence de sa définition extérieure qui a été formulée dans le chapitre 1.

Soit un groupe G engendré par ses sous-groupes normaux G_i; chaque élément g de G se laisse écrire sous la forme (8), où les symboles $i_1, \ldots, i_m$ sont tous distincts et les facteurs différents de l'unité se laissent définir d'une façon unique par l'élément g. On dit alors que *le groupe G se décompose en produit direct de ses sous-groupes G_i*. Il est évident que le groupe G se décompose en produit direct de ses sous-groupes G_i si et seulement si G est isomorphe au produit direct des groupes abstraits G_i. Pour cette raison, la notation (7) utilisée pour le groupe G décomposable en produit direct de sous-groupes G_i est la même que pour le produit direct de groupes abstraits G_i. En notation additive, on parle de la *décomposition en somme directe* et l'on écrit

$$G = G_1 \oplus \ldots \oplus G_m, \quad G = \sum_{i \in I} G_i.$$

4.3.1. Exemples. I. Le groupe additif du corps $\mathbb{C}$ se décompose en somme directe du sous-groupe des nombres réels et du sous-groupe des nombres imaginaires purs: $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$.

II. On a évidemment

$$\mathbb{Q}^* = (-1) \times \prod_p (p).$$

III. Le 4-groupe de Klein se décompose en produit direct de deux sous-groupes du second ordre :

$$\{1, (12)(34), (13)(24), (14)(23)\} = ((12)(34)) \times ((13)(24)).$$

IV. On a évidemment

$$\mathbf{D}_n(K) = G_1 \times \ldots \times G_n,$$

où G_i est un sous-groupe de $\mathbf{D}_n(K)$, dont chaque matrice a ses éléments diagonaux 1 sauf l'élément en position i.

4.3.2. Exercice. Un groupe G se décompose en produit direct de ses sous-groupes normaux G_i si et seulement si G est engendré par les G_i et toute relation $g_{i_1} \ldots g_{i_m} = e$ donne lieu aux relations $g_{i_1} = \ldots = g_{i_m} = e$. ($g_i \in G_i$, tous les symboles sont différents.)

4.3.3. Exercice. Un groupe G se décompose en produit direct de ses sous-groupes normaux G_i si et seulement si G est engendré par les G_i et

$$G_i \cap \mathrm{gr}\,(G_j \mid j \neq i) = 1 \text{ pour tout } i.$$

4.3.4. Exercice. Un groupe cyclique d'ordre mn, où m et n sont premiers entre eux, se décompose en produit direct de ses sous-groupes d'ordres m, n.

4.3.5. Exercice. Soit p un nombre premier. Un groupe cyclique d'ordre p^n ne peut pas être décomposé en produit direct de ses sous-groupes.

4.3.6. Exercice. Le groupe additif du corps $\mathbb{Q}$ ne peut pas être décomposé en produit direct de ses sous-groupes.

Un sous-groupe A du produit direct (7) s'appelle *produit sous-direct* des groupes G_i si la projection de A sur chaque facteur G_i se confond avec G_i tout entier. Soulignons que le produit sous-direct ne se définit pas par ses facteurs d'une façon unique. Il est évident que chaque sous-groupe du produit direct est produit sous-direct de ses projections. Ce n'est pas toujours un produit direct : un contre-exemple est fourni par la diagonale D du carré direct $G \times G$, qui est constituée par des couples $\langle g, g \rangle$, $g \in G$.

4.3.7. Exercice. Soient un groupe $G = G_1 \times G_2$, A un sous-groupe de G, A_i sa projection sur le facteur G_i, $i = 1, 2$. Montrer que A se décompose en produit direct $A_1 \times A_2$ si et seulement si $A_i = G_i \cap A$, $i = 1, 2$.

4.3.8. Exercice. Soit $G = G_1 \times G_2$, où G_1, G_2 sont des groupes finis d'ordres premiers entre eux. Tout sous-groupe $A \leqslant G$ se décompose en produit direct de ses projections sur les facteurs G_1, G_2.

Si G est produit sous-direct de groupes finis, il est évident que tout ensemble fini d'éléments de G est contenu dans un sous-groupe normal fini. Cette propriété caractérise les groupes qui s'appellent *localement normaux*. L'exemple du groupe $\mathbb{C}_{p^\infty}$ montre que la classe des groupes localement normaux est plus vaste que celle des produits sous-directs de groupes finis. Il existe néanmoins des liens étroits entre ces classes, cf. Ph. Hall, *J. London Math. Soc.*, 1959, **34**, p. 289-304, et Iou. M. Gortchakov, *Matem. sb.*, 1965, 67, p. 244-254. L'ouvrage de Iou. M. Gortchakov [11] expose la théorie des groupes localement normaux et plus généralement des groupes aux classes de conjugaison finies.

Par analogie aux produits sous-directs, on définit les produits sous-cartésiens : un sous-groupe A du produit cartésien

$$G = \prod_{i \in I} G_i$$

est appelé *produit sous-cartésien* des groupes G_i si la projection de A sur tout facteur G_i se confond avec G_i tout entier. Il est évident que tout produit sous-direct des groupes G_i est en même temps produit sous-cartésien de ces groupes.

4.3.9. Théorème (Remak). *Soient dans un groupe G une famille de ses sous-groupes normaux H_i, $i \in I$, et leur intersection H. Le groupe quotient G/H est isomorphe à un produit sous-cartésien de groupes quotients G/H_i.*

Démonstration. Considérons l'application

$$\varphi : G \to \prod_{i \in I} (G/H_i)$$

qui fait correspondre à chaque g de G une fonction f telle que $f(i) = gH_i$. On vérifie aisément que φ est un homomorphisme et H son noyau. Il ne reste qu'à appliquer le théorème des homomorphismes 4.2.2.

4.3.10. Exemples. I. Le groupe $\mathbb{Q}/\mathbb{Z}$ est isomorphe à une somme sous-cartésienne de groupes $\mathbb{Q}/\mathbb{Q}_p$, prise sur tous les p premiers.

II. Le groupe $\mathbb{C}^*$ est isomorphe à un produit sous-direct des groupes $\mathbb{C}^*/\mathbb{C}_{p^\infty}$ pour deux p premiers distincts quelconques.

III. Soit un ensemble M subdivisé en parties disjointes M_i, $i \in I$. Soit $G \leqslant \mathrm{S}(M)$, chaque élément de G renvoyant chaque M_i sur lui-même. Le groupe G est isomorphe à un produit sous-cartésien de sous-groupes de $\mathrm{S}(M_i)$, $i \in I$.

IV. Le groupe $\mathrm{GL}_n(\mathbb{Z})$ est isomorphe à un sous-groupe du produit cartésien des groupes finis $\mathrm{GL}_n(\mathbb{Z}_m)$, $m = 1, 2, \ldots$

4.3.11. Exercice. L'intersection des sous-groupes normaux qui définissent des groupes quotients abéliens définit elle-même un groupe quotient abélien.

4.4. **Matriochkas.** Soit G un groupe. Un système de sous-groupes de G emboîtés, contenant le sous-groupe unité et G tout entier s'appelle *matriochka* [1]) du groupe G (on dit aussi série, chaîne, suite). Avant le § 22, nous aurons affaire seulement à des matriochkas finies (sauf en deux cas particuliers, § 7 et § 13, où il s'agira de « matriochkas transfinies croissantes »), aussi le terme « matriochka » sous-entendra-t-il, jusqu'au § 22, une matriochka finie. La matriochka

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G \tag{9}$$

est dite *normale* si chaque sous-groupe G_i est normal dans G. Par exemple, toute matriochka d'un sous-groupe d'un groupe abélien est normale. Elle s'appelle *sous-normale* si elle vérifie une condition moins restrictive : chaque terme précédent est un sous-groupe normal du terme suivant, i.e. $G_i \trianglelefteq G_{i+1}$ pour $i = 0, 1, \ldots, n-1$. Les termes des matriochkas sous-normales sont appelés *sous-groupes sousnormaux* (si le sous-groupe H est sous-normal dans G, on écrit $H \triangleleft G$). Les groupes quotients G_{i+1}/G_i sont appelés *sections* de la matriochka (9). D'une façon générale, on entend par *section* de G tout groupe quotient B/A, où A, B sont deux sous-groupes de G tels que $A \trianglelefteq B$. Les matriochkas s'écrivent parfois non dans l'ordre croissant de 1 à G mais dans l'ordre décroissant de G à 1. Découvrant dans le groupe une matriochka sous-normale dont les sections sont bien connues, nous faisons un pas important dans l'étude du groupe lui-même.

On dit que le groupe G est une *extension* du groupe A par le groupe B s'il existe dans G un sous-groupe normal H tel que $H \simeq A$, $G/H \simeq B$. De ce point de vue, les sections de la matriochka sous-normale sont des blocs constitutifs qui permettent de reconstituer le groupe dans son ensemble par extensions successives. Soulignons cependant que le résultat ne se définit pas seulement par les sections utilisées mais aussi par le procédé d'assemblage employé : par exemple, l'extension de $\mathbb{Z}_2$ par $\mathbb{Z}_2$ peut donner à la fois $\mathbb{Z}_2 \times \mathbb{Z}_2$ et $\mathbb{Z}_4$. Les groupes assemblés à partir de sections cycliques sont dits *polycycliques*. Plus exactement, une matriochka sous-normale aux sections cycliques s'appelle *polycyclique* et un groupe possédant une telle matriochka, *groupe polycyclique*.

4.4.1. Exemples. I. Les sections de la matriochka $1 < (2) < \mathbb{Z} < \mathbb{Q}_p$ sont isomorphes respectivement aux groupes $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{C}_{p^\infty}$.

---

[1]) Poupée gigogne en bois, article traditionnel de l'artisanat russe. (*N. d. T.*)

II. Toutes les sections de la matriochka $1 < C_p < C_{p^2} < \ldots < C_{p^n}$ sont cycliques d'ordre p.

III. Le groupe A_4 possède une matriochka polycyclique

$$1 < \{1, (12)(34)\} < \{1, (12)(34), (13)(24), (14)(23)\} < A_4 \tag{10}$$

aux sections d'ordres 2, 2, 3. Cette matriochka n'est pas normale, car le sous-groupe ((12) (34)) n'est pas normal (bien qu'il soit sous-normal) dans A_4.

IV. Le groupe $T_n(K)$ possède une matriochka normale

$$T_n(K) \geqslant UT_n^1(K) \geqslant UT_n^2(K) \geqslant \ldots \geqslant UT_n^n(K) = 1 \tag{11}$$

aux sections $S_0, S_1, \ldots, S_{n-1}$, où

$$S_0 \simeq K^* \times \ldots \times K^* \ (n \text{ fois}),$$

$$S_m \simeq K \oplus \ldots \oplus K \quad (n - m \text{ fois}) \text{ pour } m \geqslant 1.$$

Une matriochka (sous-)normale d'un groupe induit des matriochkas (sous-)normales dans les sous-groupes et les groupes quotients:

4.4.2. Théorème. *Soit G un groupe possédant une matriochka (sous-) normale* (9). *Si $H \leqslant G$, l'intersection de* (9) *et de H nous donne une matriochka (sous-)normale dans H:*

$$1 = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_n = H, \quad H_i = G_i \cap H,$$

la section H_{i+1}/H_i étant isomorphe à un sous-groupe de la section G_{i+1}/G_i. Si $H \trianglelefteq G$, les images des termes de la matriochka (9) *par l'homomorphisme canonique $G \to G/H$ nous donnent une matriochka (sous-)normale dans G/H:*

$$1 = \bar{G}_0 \leqslant \bar{G}_1 \leqslant \ldots \leqslant \bar{G}_n = G/H, \quad \bar{G}_i = G_iH/H,$$

la section $\bar{G}_{i+1}/\bar{G}_i$ étant une image homomorphe de la section G_{i+1}/G_i.

Démonstration. Les relations $H_i \trianglelefteq H_{i+1}$, $\bar{G}_i \leqslant \bar{G}_{i+1}$ (et $H_i \trianglelefteq H$, $\bar{G}_i \trianglelefteq \bar{G}$ pour les matriochkas normales) se vérifient immédiatement. Utilisant ensuite le théorème des homomorphismes, nous obtenons

$$H_{i+1}/H_i = H_{i+1}/H_{i+1} \cap G_i \simeq H_{i+1}G_i/G_i \leqslant G_{i+1}/G_i,$$

$$\bar{G}_{i+1}/\bar{G}_i \simeq G_{i+1}H/G_iH \simeq G_{i+1}/G_i\,(G_{i+1} \cap H) \simeq (G_{i+1}/G_i)/(\ldots).$$

Le théorème est démontré.

4.4.3. Exercice. Les sous-groupes et les groupes quotients d'un groupe polycyclique sont polycycliques. L'extension d'un grou-

pe polycyclique par un groupe polycyclique est encore un groupe polycyclique. Le produit de deux sous-groupes normaux polycycliques d'un groupe quelconque est un sous-groupe polycyclique.

Deux matriochkas sous-normales d'un groupe donné sont dites *isomorphes* si elles ont même nombre de sections et si leurs sections sont liées par une correspondance biunivoque conformément à laquelle les sections correspondantes sont isomorphes. Par exemple, dans le groupe C_{12} les matriochkas

$$1 < C_2 < C_4 < C_{12}$$

et

$$1 < C_3 < C_6 < C_{12}$$

sont isomorphes. Si une matriochka contient tous les termes d'une autre, on dit qu'elle est *plus fine* que la deuxième; on dit aussi que la première est une *subdivision* de la deuxième.

4.4.4. Théorème (Schreier). *Dans un groupe quelconque, deux matriochkas (sous-)normales quelconques admettent des subdivisions (sous-)normales isomorphes.*

Démonstration. Soient dans le groupe G deux matriochkas (sous-)normales

$$1 = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_m = G, \tag{12}$$

$$1 = B_0 \leqslant B_1 \leqslant \ldots \leqslant B_n = G. \tag{13}$$

Nous subdiviserons chaque intervalle $A_i \leqslant A_{i+1}$ de la première matriochka en y intercalant une pièce fabriquée au moyen de la deuxième matriochka, et inversement. A cet effet, faisons l'intersection de la matriochka (13) avec A_{i+1} et multiplions-la ensuite terme à terme par A_i; on obtient une chaîne de sous-groupes commençant par A_i et finissant par A_{i+1}. Cette pièce intercalaire s'écrit comme suit:

$$A_i = C_{i0} \leqslant C_{i1} \leqslant \ldots \leqslant C_{in} = A_{i+1},$$
$$C_{ij} = (A_{i+1} \cap B_j)\, A_i.$$

Les pièces intercalaires pour la deuxième matriochka s'écrivent d'une façon analogue:

$$B_j = D_{j0} \leqslant D_{j1} \leqslant \ldots \leqslant D_{jm} = B_{j+1},$$
$$D_{ji} = (B_{j+1} \cap A_i)\, B_j.$$

Il est évident que si les termes des matriochkas (12), (13) étaient normaux dans G, tous les termes des pièces intercalaires le sont également. Il reste à vérifier que

$$C_{i,j+1}/C_{ij} \simeq D_{j,i+1}/D_{ji}.$$

Or, on a en vertu du théorème 4.2.4

$$C_{i,j+1}/C_{ij} = (A_{i+1} \cap B_{j+1})\, A_i/(A_{i+1} \cap B_j)\, A_i \simeq$$
$$\simeq (A_{i+1} \cap B_{j+1})/(A_{i+1} \cap B_j)\ (A_i \cap B_{j+1}),$$
$$D_{i,+1}/D_{ji} = (B_{j+1} \cap A_{i+1})\, B_j/(B_{j+1} \cap A_i)\, B_j \simeq$$
$$\simeq (B_{j+1} \cap A_{i+1})/(B_{j+1} \cap A_i)\ (B_j \cap A_{i+1}).$$

Le théorème est démontré.

Il ressort de ce théorème, en particulier, que *dans un groupe quelconque, deux matriochkas (sous-)normales quelconques sans termes répétés, qui n'ont aucune subdivision sans termes répétés sont isomorphes* (théorème de Jordan-Hölder).

4.4.5. Exercice. Soit G un groupe polycyclique. Toutes ses matriochkas polycycliques ont même nombre de sections infinies, nombre que l'on appelle *dimension polycyclique* de G. Il est commode de raisonner par récurrence sur la dimension polycyclique en étudiant les groupes polycycliques.

Remarquons que les théorèmes 4.4.2 et 4.4.4 restent parfaitement vrais pour les matriochkas dénombrables de la forme

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n \ldots, \quad G = \bigcup_{n=1}^{\infty} G_n,$$

ainsi que pour certains types plus compliqués de « matriochkas sous-normales infinies »; or, comme nous l'avons déjà dit, ce sujet ne sera pas abordé avant le § 22.

Avant de terminer ce n°, nous devons indiquer la notion d'approximabilité, étroitement liée aux homomorphismes. Sous sa forme la plus générale, cette notion se définit comme suit (M. I. Kargapolov, Iou. I. Merzliakov. *Groupes infinis*. In : *Bilan des recherches. Algèbre. Topologie Géométrie.* 1966. Moscou, 1968 (en russe), p. 75 ; nous parlons des groupes, mais nous pourrions parler de n'importe quelles structures algébriques, cf. n° 27.1 de l'Appendice).

Soient G un groupe et ρ une relation (ou prédicat) entre éléments et ensembles d'éléments, définie sur G et sur toutes ses images homomorphes (par exemple, les relations binaires « égal à l'élément . . . », « appartient à un sous-groupe . . . », « est le conjugué de . . . », etc.). Soit K une classe de groupes. Nous disons que le groupe G *se laisse approcher* (ou *admet une approximation*) *par des groupes de K par rapport à* ρ si, pour n'importe quels éléments et ensembles d'éléments de G ne vérifiant pas ρ, il existe un homomorphisme de G sur un groupe de K, tel que les images de ces éléments ne vérifient pas ρ, elles non plus. Dans la littérature, on parle le plus souvent de l'approximabilité par rapport à l'égalité des éléments : dans ce cas,

on omet généralement d'indiquer la relation et l'on parle de l'approximabilité tout court. Il ressort du théorème de Remak 4.3.9 qu'un groupe G se laisse approcher par des groupes de la classe K si et seulement si G peut être plongé dans le produit cartésien des groupes de K.

L'approximabilité par des groupes finis est appelée aussi *finitude résiduelle*. Il est commode de désigner la finitude résiduelle par rapport au prédicat ρ par le symbole RFρ ; en particulier, si ρ parcourt les prédicats « égal à », « conjugué de », « appartient à un sous-groupe de type fini », « appartient à un sous-groupe donné H », etc., on obtient les propriétés (et les classes) RFEg, RFConj, RFAp, RFAp$_\omega$, RFAp-H, etc. L'importance de ces propriétés a été soulignée par A. I. Maltsev (*Outch. zap. Ivanovskogo ped. in-ta*, 1958, 18, p. 49-60) : leur existence dans le groupe définit la résolubilité du problème algorithmique correspondant.

§ 5. Endomorphismes. Automorphismes

5.1. Définitions. Une application homomorphe d'un groupe dans lui-même est son *endomorphisme*, et une application isomorphe d'un groupe sur lui-même est son *automorphisme*. L'image endomorphe est analogue à la carte d'identité que l'on a dans sa poche. Les ensembles de tous les endomorphismes et automorphismes d'un groupe donné G se notent par End G et Aut G respectivement. On munit ces ensembles de l'opération de multiplication en assimilant le produit de deux endomorphismes à leur réalisation successive. On vérifie aisément que End G devient alors un demi-groupe et Aut G tout un groupe, et ceci de sorte que

$$\mathrm{Aut}\ G \leqslant \mathrm{S}(G).$$

Si G est un groupe abélien, on munit l'ensemble End G également de l'opération d'addition en posant

$$x^{\varphi+\psi} = x^{\varphi}x^{\psi} \text{ pour } \varphi,\ \psi \in \mathrm{End}\ G, \quad x \in G$$

On vérifie immédiatement que End G devient alors un anneau. Or, dans le cas général, End n'est pas un anneau et joue en théorie des groupes un rôle moins important que Aut.

Nous avons déjà indiqué dans le chapitre 1 que la conjugaison de G par un élément a de G est un isomorphisme, car elle est biunivoque et

$$(xy)^a = x^a y^a \text{ pour } x,\ y \in G$$

Cet automorphisme $\hat{a}$ s'appelle *automorphisme intérieur* du groupe G opéré par l'élément a. On vérifie immédiatement que

$$(x^a)^b = x^{ab}, \quad (x^a)^{a^{-1}} = x, \quad x^{\varphi^{-1}\hat{a}\varphi} = x^{\widehat{a^\varphi}},$$
$$a, b, x \in G, \quad \varphi \in \operatorname{Aut} G,$$

d'où

$$\hat{a}\hat{b} = \widehat{ab}, \quad \hat{a}^{-1} = \widehat{a^{-1}}, \quad \varphi^{-1}\hat{a}\varphi = \widehat{a^\varphi}. \tag{1}$$

Il en découle en particulier que l'ensemble Int G de tous les automorphismes intérieurs du groupe G est un sous-groupe normal du groupe Aut G,

$$\operatorname{Int} G \leqslant \operatorname{Aut} G. \tag{2}$$

Les automorphismes non intérieurs sont appelés *extérieurs*, et le groupe

$$\operatorname{Out} G = \operatorname{Aut} G/\operatorname{Int} G \tag{3}$$

est appelé *groupe des automorphismes extérieurs*. Pour un groupe abélien, Out se confond évidemment avec Aut.

La première des relations (1) permet de voir que l'application $G \to \operatorname{Int} G$ qui fait correspondre à chaque g de G un automorphisme intérieur $\hat{g}$ est homomorphe. Le noyau de cet homomorphisme est constitué d'éléments g tels que

$$x^g = x, \quad x \in G,$$

i.e. se confond avec le centre $Z(G)$ du groupe G. En appliquant le théorème des homomorphismes, on obtient la formule

$$\operatorname{Int} G \simeq G/Z(G). \tag{4}$$

A titre d'illustration, décrivons les anneaux End G et les groupes Aut G, pour quelques groupes G proposés dans les exemples I à IV du chapitre 1, employant à cet effet la formule évidente

$$(\operatorname{End} G)^* = \operatorname{Aut} G.$$

5.1.1. Exemples. I. On a

$$\operatorname{End} \mathbf{Z} \simeq \mathbf{Z}, \quad \operatorname{Aut} \mathbf{Z} \simeq \mathbf{Z}^* \simeq \mathbf{Z}_2, \tag{5}$$
$$\operatorname{End} \mathbf{Z}_m \simeq \mathbf{Z}_m, \quad \operatorname{Aut} \mathbf{Z}_m \simeq \mathbf{Z}_m^*, \tag{6}$$
$$\operatorname{End} \mathbb{Q} \simeq \mathbb{Q}, \quad \operatorname{Aut} \mathbb{Q} \simeq \mathbb{Q}^*. \tag{7}$$

En effet, les isomorphismes pour End se déterminent respectivement par

$$\varphi \to 1\varphi, \quad \varphi \to (1 \pmod m)\,\varphi, \quad \varphi \to 1\varphi$$

(en notation additive, l'endomorphisme φ s'écrit en facteur et non en exposant). Examinons le dernier cas en détail. Le caractère homomorphe de l'application $\varphi \to 1\varphi$ est immédiat. Montrons que le noyau est trivial, i.e. que $1\varphi = 0$ entraîne $\varphi = 0$. Soient r, s deux entiers relatifs, $s \neq 0$. Puisque

$$0 = 1\varphi = \left(s \cdot \frac{1}{s}\right)\varphi = s\left(\frac{1}{s}\right)\varphi,$$

il vient

$$\left(\frac{1}{s}\right)\varphi = 0, \quad \left(\frac{r}{s}\right)\varphi = 0, \quad \varphi = 0.$$

Enfin, pour tout $\alpha \in \mathbb{Q}$ on trouve une image réciproque $\varphi \in \operatorname{End} \mathbb{Q}$, à savoir l'endomorphisme $x \to x\alpha$ du groupe $\mathbb{Q}$.

II. Décrivons l'anneau End $\mathbb{C}_{p^\infty}$. Soit ε_n une racine primitive p^n-ième de 1 du corps des nombres complexes, avec $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1, 2, \ldots$ Il est évident que les endomorphismes du groupe $\mathbb{C}_{p^\infty}$ se définissent complètement par leur action sur $\varepsilon_1, \varepsilon_2, \ldots$ Soit $\varphi \in \operatorname{End} \mathbb{C}_{p^\infty}$; on a alors

$$\varepsilon_n^\varphi = \varepsilon_n^{k_n}, \quad k_n \in \mathbb{Z}_{p^n}, \quad n = 1, 2, \ldots$$

Puisque $(\varepsilon_{n+1}^\varphi)^p = \varepsilon_n^\varphi$, k_n est l'image de k_{n+1} par l'homomorphisme $\mathbb{Z}_{p^{n+1}} \to \mathbb{Z}_{p^n}$ (régi par la loi : $x \pmod{p^{n+1}} \to x \pmod{p^n}$ pour $x \in \mathbb{Z}$). A tout φ de End $\mathbb{C}_{p^\infty}$ est associée donc une suite $(k_1, k_2, \ldots)$, $k_n \in \mathbb{Z}_{p^n}$, où k_n est l'image de k_{n+1} par l'homomorphisme canonique $\mathbb{Z}_{p^{n+1}} \to \mathbb{Z}_{p^n}$. On vérifie immédiatement que l'ensemble $\mathbb{Z}_{p^\infty}$ de toutes ces suites est un anneau par rapport aux opérations d'addition et de multiplication effectuées composante par composante, et que l'application obtenue End $\mathbb{C}_{p^\infty} \to \mathbb{Z}_{p^\infty}$ est un isomorphisme. La description de l'anneau End $\mathbb{C}_{p^\infty}$ est terminée. L'anneau $\mathbb{Z}_{p^\infty}$ est appelé *anneau des entiers p-adiques*; ses éléments s'écrivent de façon naturelle sous la forme

$$\ldots a_n \ldots a_1 a_0 = \sum_{n=0}^{\infty} a_n p^n, \quad 0 \leqslant a_n < p,$$

et s'additionnent et se multiplient de façon tout aussi naturelle: « on pose le résidu et l'on retient le nombre de périodes ». Citons à

titre d'illustration quelques exemples d'opérations sur les entiers 5-adiques:

$$\begin{array}{r} +\begin{array}{r}\ldots 20134\\ \ldots 12203\end{array}\\ \hline \ldots 32342 \end{array} \qquad \begin{array}{r} \times\begin{array}{r}\ldots 20134\\ \ldots 12203\end{array}\\ \hline \ldots 11012\\ \ldots 0000\\ \ldots 323\\ +\ldots 23\\ \ldots 4\\ \ldots\\ \hline \ldots 11312 \end{array} \qquad \begin{array}{r} -\begin{array}{r}\ldots 20134\\ \ldots 12203\end{array}\\ \hline \ldots 02431 \end{array}$$

Notons en passant que l'ensemble $\mathbb{Q}_{p^\infty}$ des nombres p-adiques « fractionnaires » de la forme

$$\ldots a_n \ldots a_1 a_0, a_{-1} \ldots a_{-s} = \sum_{n=-s}^{\infty} a_n p^n, \quad 0 \leqslant a_n < p,$$

a déjà une structure de corps par rapport aux opérations analogues et s'appelle *corps des nombres p-adiques*. Nous laissons au lecteur le soin d'établir la règle de division par tranches des nombres p-adiques (la division est la seule opération pour laquelle p doit être un nombre premier). Donc,

$$\operatorname{End} \mathbb{C}_{p^\infty} \simeq \mathbb{Z}_{p^\infty}, \quad \operatorname{Aut} \mathbb{C}_{p^\infty} \simeq \mathbb{Z}^*_{p^\infty}. \tag{8}$$

On comprend facilement que $\mathbb{Z}^*_{p^\infty}$ est constitué des entiers p-adiques dont le « terme constant » a_0 est non nul.

III. On a la formule

$$\operatorname{Aut} \mathbf{S}_n \simeq \mathbf{S}_n \quad \text{pour} \quad n \neq 2, 6. \tag{9}$$

Nous la démontrerons en fin du paragraphe. Pour $n = 2, 6$ cette formule cesse d'être vraie, voir ibid.

IV. Une littérature abondante est consacrée à la description des automorphismes des groupes matriciels classiques (voir par exemple [1], [9]). Citons sans démonstration un résultat typique. Soient $n \geqslant 3$ et K un corps commutatif de caractéristique $\neq 2$. Pour tout automorphisme φ de $\operatorname{Aut} \mathbf{GL}_n(K)$, on a alors soit

$$x^\varphi = x^\psi \cdot g^{-1} x^\sigma g, \quad x \in \mathbf{GL}_n(K), \tag{10}$$

soit

$$x^\varphi = x^\psi \cdot g^{-1} x^\sigma g, \quad x \in \mathbf{GL}_n(K), \tag{11}$$

en choisissant convenablement $\sigma \in \operatorname{Aut} K$, $\psi\colon \mathbf{GL}_n(K) \to K^*$ et un élément $g \in \mathbf{GL}_n(K)$. Le symbole ^ signifie ici qu'on doit pren-

dre l'inverse de la transposée de la matrice donnée. Pour un grand nombre de groupes matriciels, surtout sur les anneaux, les groupes d'automorphismes sont encore mal connus ou n'ont jamais été étudiés.

5.1.2. Exercice. Si $|G| > 2$, on a $\operatorname{Aut} G \neq 1$.
Indication. Considérer les cas où
1° G est non abélien,
2° G est abélien et contient des éléments d'ordre > 2,
3° G vérifie la relation identique $x^2 = e$.

5.1.3. Exercice:

$$\operatorname{End}(\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}) \simeq \mathrm{M}_n(\mathbf{Z}),$$
$$\operatorname{Aut}(\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}) \simeq \mathrm{GL}_n(\mathbf{Z}),$$
$$\operatorname{End}(\mathbf{Z}_m \oplus \ldots \oplus \mathbf{Z}_m) \simeq \mathrm{M}_n(\mathbf{Z}_m),$$
$$\operatorname{Aut}(\mathbf{Z}_m \oplus \ldots \oplus \mathbf{Z}_m) \simeq \mathrm{GL}_n(\mathbf{Z}_m),$$
$$\operatorname{End}(\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}) \simeq \mathrm{M}_n(\mathbb{Q}),$$
$$\operatorname{Aut}(\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}) \simeq \mathrm{GL}_n(\mathbb{Q})$$

(il y a n termes dans les premiers membres).

5.1.4. Exercice:

$$\operatorname{End}(\mathrm{C}_{p^\infty} \times \ldots \times \mathrm{C}_{p^\infty}) \simeq \mathrm{M}_n(\mathbf{Z}_{p^\infty}),$$
$$\operatorname{Aut}(\mathrm{C}_{p^\infty} \times \ldots \times \mathrm{C}_{p^\infty}) \simeq \mathrm{GL}_n(\mathbf{Z}_{p^\infty})$$

(il y a n facteurs dans les premiers membres).

5.1.5. Exercice. Tous les sous-groupes de congruence

$$\mathrm{GL}_n(\mathbf{Z}_{p^\infty}, \quad p^k\mathbf{Z}_{p^\infty}), \quad k = 1, 2, \ldots,$$

du groupe $\mathrm{GL}_n(\mathbf{Z}_{p^\infty})$ sont sans torsion, à l'exception du cas où $p = 2$, $k = 1$.

Indication. Examiner la formule du binôme

$$(e + p^k a)^m = e + \binom{m}{1} p^k a + \binom{m}{2} p^{2k} a^2 + \ldots + p^{mk} a^m.$$

5.1.6. Exercice. Soient A, B deux groupes abéliens. L'ensemble de tous les homomorphismes $\operatorname{Hom}(A, B)$ de A dans B est un groupe abélien par rapport à l'addition point par point régie par la loi

$$a(\varphi + \psi) = a\varphi + a\psi, \quad a \in A,$$

tandis que pour $A = B$ il est un anneau par rapport à l'addition point par point et à la superposition assimilée à la multiplication:

$$a(\varphi\psi) = (a\varphi)\psi, \quad a \in A.$$

5.1.7. Exercice. Se rappelant que les ordres des éléments d'un groupe restent inchangés par ses automorphismes, énumérer les automorphismes du groupe S_3 et vérifier qu'ils sont tous intérieurs.

5.2. Sous-groupes permis. Le langage des automorphismes permet de donner une autre définition de sous-groupe normal : un sous-groupe H d'un groupe G est normal si et seulement si H admet tous les automorphismes intérieurs de G, i.e. si

$$H^{\varphi} \leqslant H \text{ pour tout } \varphi \in \operatorname{Int} G.$$

Remplaçant dans cette condition Int G par un ensemble arbitraire Φ contenu dans End G, on aboutit à une notion plus générale : un sous-groupe H d'un groupe G est dit *permis* par rapport à Φ (ou Φ-*permis*) et se note $H \overset{\Phi}{\leqslant} G$ si

$$H^{\varphi} \leqslant H \text{ pour tout } \varphi \in \Phi.$$

Il est évident que le sous-groupe unité et le groupe tout entier sont permis par rapport à Φ quelconque. Si le groupe ne contient aucun autre sous-groupe normal Φ-permis, on dit que le groupe est Φ-*simple*. Pour $\varphi \in \Phi$ les parties M et M^{φ} sont appelées Φ-*conjuguées*. La relation de Φ-conjugaison n'intervient que pour $\Phi \leqslant \operatorname{Aut} G$, auquel cas elle devient équivalence ; dans le cas général, cette relation est inutile. Dans les cas les plus répandus où Φ se confond avec End G, Aut G ou Int G, le préfixe Φ- se lit respectivement End-, ou « par rapport aux endomorphismes » ; Aut-, ou « par rapport aux automorphismes » ; Int-, ou « intérieurement », ou « par rapport aux automorphismes intérieurs », et l'on emploie les notations

$$H \overset{e}{\leqslant} G, \quad H \overset{a}{\leqslant} G, \quad H \overset{i}{\leqslant} G.$$

Au lieu de la notation $\overset{i}{\leqslant}$, on utilise généralement le symbole stylisé $\trianglelefteq$ que nous avons introduit dès le début. Remarquons que certains auteurs emploient des termes particuliers pour désigner les Φ-notions, à savoir :

	intérieurement	par rapport aux automorphismes	par rapport aux endomorphismes
conjugués	conjugués	isotypes	—
permis	normaux	caractéristiques	complètement caractéristiques
simples	simples	élémentaires	—

Par pitié, nous épargnerons au lecteur toute cette terminologie; seuls seront utilisés, dans cet ouvrage, les qualificatifs *conjugué*, *normal* et *simple*, les autres étant cités à titre de référence.

5.2.1. Exercice. L'intersection et l'engendrement d'une famille quelconque de sous-groupes Φ-permis est un sous-groupe Φ-permis.

5.2.2. Exercice. Les relations $\overset{e}{\leqslant}$, $\overset{a}{\leqslant}$ sont transitives (à la différence de la relation $\trianglelefteq$), i.e.

$$A \overset{e}{\leqslant} B, \quad B \overset{e}{\leqslant} C \Rightarrow A \overset{e}{\leqslant} C,$$

$$A \overset{a}{\leqslant} B, \quad B \overset{a}{\leqslant} C \Rightarrow A \overset{a}{\leqslant} C.$$

5.2.3. Exercice. Un sous-groupe Aut-permis d'un sous-groupe normal est normal dans le groupe tout entier, i.e.

$$A \overset{a}{\leqslant} B, \quad B \trianglelefteq C \Rightarrow A \trianglelefteq C.$$

Des exemples évidents de sous-groupes End-permis d'un groupe arbitraire G sont fournis par ses commutants successifs, *sa puissance n-ième* $G^n = \mathrm{gr}\,(x^n \mid x \in G)$ et sa *n-ième couche* $G_n = \mathrm{gr}\,(x \mid x \in G, x^n = 1)$. Le centre d'un groupe G est toujours Aut-permis, car de $ab = ba$, $a, b \in G$, $\varphi \in \mathrm{Aut}\, G$, il ressort que $a^\varphi b^\varphi = b^\varphi a^\varphi$; remarquons que l'élément a^φ parcourt le groupe G tout entier en même temps que l'élément a. Soulignons que, même dans un groupe fini, le centre n'est pas toujours End-permis (voir l'exemple 5.2.4. III).

Donnons quelques exemples de sous-groupes permis dans des groupes concrets.

5.2.4. Exemples. I. Dans les groupes $\mathbb{Z}$, $\mathbb{Z}_n$, tout sous-groupe est End-permis. Le groupe $\mathbb{Q}$ est Aut-simple (et *a fortiori* End-simple), car tous ses éléments non nuls sont Aut-conjugués deux à deux, voir la définition de Aut $\mathbb{Q}$ dans les pages précédentes.

II. Il est évident que

$$\mathbb{C}_p \overset{e}{\leqslant} \mathbb{C}_{p^2} \overset{e}{\leqslant} \ldots, \quad \mathbb{C}_{p^n} \overset{e}{\leqslant} \mathbb{C}_{p^\infty}.$$

III. Puisque le commutant d'un groupe est End-permis dans ce groupe, on a $\mathbf{A}_n \overset{e}{\leqslant} \mathbf{S}_n$. Soit $n \geqslant 3$. Puisque le groupe $\mathbf{S}_n$ est sans centre, le centre du groupe fini $\mathbb{C}_2 \times \mathbf{S}_n$ est constitué par le sous-groupe $\mathbb{C}_2$. Ce n'est pas un sous-groupe End-permis, car il n'admet pas l'endomorphisme $(-1)^m x \mapsto (12)^m$, $m = 0, 1$, $x \in \mathbf{S}_n$.

IV. Soit K un corps commutatif. Puisque le commutant réciproque de deux sous-groupes Φ-permis est un sous-groupe Φ-permis, on a

$$\mathrm{SL}_n(K) \overset{c}{\leqslant} \mathrm{GL}_n(K),$$

$$\mathrm{T}_n(K) \overset{c}{\geqslant} \mathrm{UT}_n^i(K), \quad i = 1, 2, \ldots$$

5.2.5. Exercice. Les sous-groupes primaires maximaux d'un groupe abélien sont End-permis.

5.2.6. Exercice. Le sous-groupe de Frattini d'un groupe quelconque est Aut-permis: pour cette raison, il est égal à 1 dans un groupe simple fini.

5.2.7. Exercice. Le groupe $\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}$ est Aut-simple.

5.2.8. Exercice. Un groupe abélien périodique est Aut-simple si et seulement si ce groupe est *abélien élémentaire*, i.e. un groupe abélien de période égale à un nombre premier ou, ce qui revient au même, s'il se décompose en somme directe d'une famille d'images isomorphes du groupe $\mathbb{Z}_p$ pour un p premier.

On considère parfois une situation plus générale: soient G un groupe et V un ensemble quelconque sur lequel est définie une application $V \to \mathrm{End}\, G$. L'ensemble V s'appelle alors *ensemble des opérateurs* de G, et pour $\Phi \subseteq V$ toutes les Φ-notions définies ci-dessus restent applicables. Lorsque $\Phi = V$, au lieu de Φ-, on écrit alors V- (se lit « opératoriellement », ou « par rapport aux opérateurs »).

5.3. Groupes parfaits. Un groupe est dit *parfait* s'il est sans centre et tous ses automorphismes sont intérieurs. Si le groupe G est parfait, on a $Z(G) = 1$, $\mathrm{Out}\, G = 1$ et, en vertu de (3) et (4),

$$\mathrm{Aut}\, G \simeq G.$$

Autrement dit, au lieu d'étudier le groupe d'automorphismes, on étudie le groupe lui-même. Cette propriété des groupes parfaits leur a valu leur appellation somptueuse donnée à l'aube de la théorie des groupes. En réalité, les groupes parfaits ne jouent aucun rôle privilégié en théorie des groupes (comme d'ailleurs les nombres parfaits en théorie des nombres). Le but de ce n° était d'indiquer une série classique de groupes parfaits, à savoir: les groupes symétriques.

5.3.1. Théorème (Hölder). *Pour $n \neq 2, 6$, le groupe symétrique S_n est parfait.*

Démonstration. a) Nous avons appris dans le § 3 que S_n a un centre trivial pour $n \geqslant 3$. Il reste à montrer que pour $n \neq 6$ tout automorphisme γ de S_n est intérieur. Soit B_k l'ensemble de

tous les produits de k transpositions indépendantes dans S_n, $1 \leqslant k \leqslant n/2$. Nous avons vu dans le n° 2.5.7. III que deux permutations dans S_n sont conjuguées dans S_n si et seulement si, décomposées en cycles indépendants, elles comportent un même nombre de cycles de chaque longueur donnée. En particulier, $B_1 \cup B_2 \cup \ldots$ est une partition de l'ensemble de tous les éléments d'ordre 2 de S_n en classes de conjugaison ; les automorphismes intérieurs de S_n renvoient chaque B_k sur lui-même. Cela nous suggère le procédé suivant : nous montrerons d'abord que B_1 est renvoyé sur lui-même par γ, et ensuite, que γ est un automorphisme intérieur.

b) L'automorphisme γ applique B_1 sur lui-même. En effet, tout automorphisme d'un groupe conserve les ordres des éléments et fait passer les classes de conjugaison en classes de conjugaison, si bien que $B_1^\gamma = B_k$ pour un k approprié. Proposons-nous de déduire l'égalité $B_1^\gamma = B_1$ par un raisonnement assez sommaire : vérifions que $|B_k| \neq |B_1|$ si $k \neq 1$, $n \neq 6$.

En effet, S_n contient $\binom{n}{2}$ transpositions ; il existe donc $\prod_{i=0}^{k-1} \binom{n-2i}{2}$ ensembles de k transpositions indépendantes. Puisque l'ordre des facteurs dans le produit de transpositions indépendantes est sans importance, on a

$$|B_k| = \frac{1}{k!} \prod_{i=0}^{k-1} \binom{n-2i}{2} = \frac{1}{k!2^k} n(n-1) \ldots (n-2k+1).$$

L'égalité $|B_1| = |B_k|$ se réduit alors à

$$(n-2)(n-3) \ldots (n-2k+1) = k!\, 2^{k-1}. \qquad (12)$$

Montrons que cette égalité cesse d'avoir lieu pour $n \neq 6$, $k \neq 1$. En effet, le second membre de (12) étant strictement positif, il doit y avoir $n \geqslant 2k$, si bien que le premier membre doit vérifier l'inégalité

$$(n-2)(n-3) \ldots (n-2k+1) \geqslant (2k-2)!.$$

On en déduit aisément par récurrence que

$$(2k-2)! > k!\, 2^{k-1} \text{ pour } k \geqslant 4.$$

Il reste à considérer les cas de $k = 2, 3$. Pour $k = 2$, on s'assure sans peine que (12) ne peut avoir lieu pour aucun n. Soit $k = 3$. Puisque $n \geqslant 2k$ et $n \neq 6$, on a $n > 6$ et

$$(n-2)(n-3) \ldots (n-2k+1) \geqslant 5 \cdot 4 \cdot 3 \cdot 2 > 3!\, 2^2 = k!\, 2^{k-1}.$$

L'égalité (12) est donc impossible pour $n \neq 6$, $k \neq 1$.

c) L'automorphisme γ est intérieur. En effet, soit $T(i)$ l'ensemble de toutes les transpositions du symbole i avec les autres symboles.

Montrons que $T(i)^\gamma = T(j)$ pour un certain j. Puisque deux transpositions quelconques de $T(i)$ sont non permutables, leurs images par γ doivent contenir aussi un symbole transposé commun. Le triplet (ia), (ib), (ic) ne peut alors passer en triplet (ju), (jv), (uv), car le produit des trois premiers éléments est d'ordre 4 et celui des trois seconds, d'ordre 2. On a donc $T(i)^\gamma \subseteq T(j)$. Appliquant à $T(j)$ l'automorphisme inverse γ^{-1}, on s'assure que $T(i)^\gamma = T(j)$. L'automorphisme γ donne ainsi une permutation π telle que $T(i)^\gamma = T(i\pi)$ pour tout $i = 1, 2, \ldots, n$. Puisque

$$(kl)^\gamma = (T(k) \cap T(l))^\gamma = T(k\pi) \cap T(l\pi) = (k\pi, l\pi) = \pi^{-1}(kl)\pi,$$

l'automorphisme γ se confond sur toutes les transpositions, donc aussi sur toutes les permutations, avec la conjugaison par la permutation π. Le théorème est démontré.

Les groupes S_2, S_6 ne sont pas parfaits, car le premier est abélien et le second admet un automorphisme extérieur d'ordre 2. La construction de cet automorphisme est décrite par exemple dans l'article de D. W. Miller, *Amer. Math. Monthly*, 1958, 65, n° 4, p. 252-254.

5.3.2. Exercice. Un sous-groupe normal parfait est toujours un facteur direct dans la décomposition de son groupe. (Question suggestive: quel est l'autre facteur?)

§ 6. Extensions par automorphismes

Décrivons deux constructions réalisées au moyen d'automorphismes, fort importantes en théorie des groupes.

6.1. **Holomorphe.** Cette construction apparaît lorsqu'on se demande si un groupe arbitraire G peut être injecté par un homomorphisme dans un groupe G^*, de façon que tout automorphisme de G soit une restriction d'un automorphisme intérieur de G^*. Soit $\Phi = \mathrm{Aut}\, G$. Il se trouve qu'on peut prendre comme G^* l'ensemble des couples φg, $\varphi \in \Phi$, $g \in G$, que l'on munit de la multiplication définie par

$$\varphi g \cdot \varphi' g' = \varphi\varphi' g^{\varphi'} g' \tag{1}$$

(nous écrivons les couples sans parenthèses ni virgules). En effet, les axiomes de groupe se vérifient immédiatement. On vérifie tout aussi immédiatement que les applications

$$\Phi \to G^*, \quad G \to G^* \tag{2}$$

régies par les lois $\varphi \mapsto \varphi 1$, $g \mapsto 1g$ sont des homomorphismes injectifs qui permettent d'identifier Φ et G à des sous-groupes de G^*. Il ressort aussitôt de la loi de multiplication (1) que

$$\varphi^{-1} g \varphi = g^{\varphi} \text{ pour } \varphi \in \Phi, \quad g \in G. \tag{3}$$

Il devient clair que

$$G^* = \Phi G, \quad G \trianglelefteq G^*, \quad \Phi \cap G = 1 \tag{4}$$

et qu'en vertu de (3) tout automorphisme $\varphi \in \Phi$ est une restriction d'un automorphisme intérieur du groupe G^*. Le problème proposé est résolu. Le groupe ΦG ainsi construit s'appelle *holomorphe* du groupe G et se note Hol G.

Lorsqu'on prend $\Phi \leqslant \operatorname{Aut} G$ au lieu de $\Phi = \operatorname{Aut} G$, le groupe ΦG conserve ses propriétés (3), (4). Dans ce cas, ΦG est appelé *extension du groupe G par le groupe d'automorphismes* Φ. Grâce à (4), cette notion se trouve en accord avec la définition générale d'une extension (n° 4.4).

On peut généraliser encore plus la situation en prenant un groupe arbitraire Φ muni d'un homomorphisme $\Phi \to \operatorname{Aut} G$. Admettant que les éléments de Φ opèrent sur G comme les automorphismes correspondants, on transforme ΦG, au moyen de la loi (1), en un groupe qui possède les propriétés (3), (4). Le groupe ΦG s'appelle alors *extension du groupe G par le groupe d'opérateurs* Φ.

Notons que toutes les extensions envisagées ci-dessus sont scindées: l'extension G d'un groupe A par un groupe B est dite *scindée* si G admet des sous-groupes H, K tels que

$$G = HK, \quad A \simeq H \trianglelefteq G, \quad H \cap K = 1.$$

Il est évident qu'on a alors $K \simeq G/A$. On dit aussi que G est *produit semi-direct* des groupes A et B et l'on écrit $G = A \rtimes B$ ou $G = B \ltimes A$.

Citons les holomorphes de quelques groupes concrets.

6.1.1. Exemples. I. Soit K n'importe lequel des anneaux $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}$. Conformément à l'exemple 5.1.1. I, chaque automorphisme du groupe additif de K se réduit à une multiplication par un élément de K^*, aussi

$$\operatorname{Hol} K \simeq \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \,\middle|\, \alpha \in K^*, \quad \beta \in K \right\}.$$

II. Une définition de forme analogue peut être donnée à Hol $\mathbb{C}_{p^\infty}$. Nous appellerons *p-filet* une suite partielle $(s_1, s_2, \ldots)$ dont quelques premières positions sont vacantes et les autres sont occupées par les éléments $s_n \in \mathbb{Z}_{p^n}$, avec $ps_n = s_{n+1}$ (au sens clair), et telle que les places vides ne peuvent être occupées sans que la propriété signalée soit compromise. Convenons de faire l'addition des p-filets composante par composante dans les positions où les deux termes

sont présents, en complétant ensuite la somme dans les positions vides chaque fois que cela est possible. On vérifie immédiatement que les p-filets ainsi additionnés forment un groupe. Ce groupe est isomorphe à $\mathbb{C}_{p^\infty}$. Soit en effet ε_n une racine primitive p^n-ième de 1 dans le corps des nombres complexes, telle que $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1, 2, \ldots$ Chaque nombre x de $\mathbb{C}_{p^\infty}$ appartient à un $\mathbb{C}_{p^n}$, aussi $x = \varepsilon_n^{s_n}$, $s_n \in \mathbb{Z}_{p^n}$, à partir d'un certain n. Puisque $\varepsilon_{n+1}^{s_{n+1}} = \varepsilon_n^{s_n} = \varepsilon_{n+1}^{p s_n}$, la suite partielle des exposants s_n sera un p-filet. On voit sans peine que l'application $x \mapsto (s_1, s_2, \ldots)$ est un isomorphisme du groupe $\mathbb{C}_{p^\infty}$ sur le groupe des p-filets ; notons que les automorphismes de Aut $\mathbb{C}_{p^\infty}$ représentés par des entiers p-adiques conformément à l'exemple 5.1.1. II, opèrent sur les p-filets comme des multiplications composante par composante. Aussi

$$\operatorname{Hol} \mathbb{C}_{p^\infty} \simeq \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \middle| \alpha \in \mathbb{Z}_{p^\infty}^*, \ \beta \text{ est un } p\text{-filet} \right\}.$$

La différence par rapport à l'exemple précédent consiste ici en ce que les coefficients des matrices sont tirés de différents ensembles sans que l'anneau sous-jacent soit indiqué.

III. Nous savons que pour $n \neq 2, 6$, le groupe $\mathbf{S}_n$ est parfait. En particulier, Aut $\mathbf{S}_n \simeq \mathbf{S}_n$. Puisque $\mathbf{S}_n$ est normal dans son holomorphe, il y constitue un facteur du produit direct (exercice 5.3.2). Donc

$$\operatorname{Hol} \mathbf{S}_n \simeq \mathbf{S}_n \times \mathbf{S}_n \quad \text{pour } n \neq 2, 6.$$

Il est clair que la formule Hol $G \simeq G \times G$ reste valable pour tout autre groupe parfait G.

IV. Pour les holomorphes des groupes **GL**, **SL**, **T**, etc., la description serait probablement aussi compliquée que la définition, vu que même les groupes d'automorphismes ont une structure assez compliquée dans les cas signalés.

6.1.2. Exercice. Soit K un des anneaux $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{C}$. Démontrer la formule

$$\operatorname{Hol}(K \oplus \ldots \oplus K) \simeq \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \middle| \alpha \in \mathbf{GL}_n(K), \ \beta \in K \oplus \ldots \oplus K \right\}$$

(les sommes contiennent n termes).

6.1.3. Exercice. Chercher toutes les classes de conjugaison dans le groupe Hol $\mathbb{Z}$.

6.1.4. Exercice. Indiquer dans Hol $\mathbb{Z}$ une suite décroissante de sous-groupes normaux

$$\operatorname{Hol} \mathbb{Z} = H_0 \geqslant H_1 \geqslant \ldots,$$

telle que $\bigcap H_i = 1$ et que chaque section H_i/H_{i+1} soit contenue dans le centre du groupe quotient H_0/H_{i+1}, $i = 0, 1, 2, \ldots$

6.1.5. Exercice. Hol $\mathbb{Z}$ est-il un groupe parfait?

6.1.6. Exercice. Soit G extension d'un p-groupe abélien élémentaire fini A par un q-groupe abélien élémentaire fini B. Si $p \neq q$ et B est un groupe non cyclique, il existe dans G des éléments d'ordre pq.

Solution. Assimilons le groupe $A \simeq \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ à un espace vectoriel sur un corps commutatif k de p éléments. Soit B^* l'ensemble des transformations linéaires de cet espace induites par les conjugaisons opérées au moyen des éléments de B. On voit sans peine que le problème se réduit à la recherche d'éléments non triviaux $a \in A$, $b \in B$ tels que $a^b = a$ (auquel cas ab sera un élément cherché d'ordre pq). Si l'homomorphisme canonique $\varphi: B \to B^*$ n'est pas un isomorphisme, la chose est claire. Par contre, si φ est un isomorphisme, on est amené à chercher dans B^* un élément θ distinct de 1 auquel correspond dans l'espace A un point fixe distinct de 0. Par définition, B^* contient deux transformations φ, ψ d'ordre q telles que gr $(\varphi) \neq$ gr (ψ). On apprend dans le cours d'algèbre générale que deux transformations linéaires permutables possèdent un vecteur propre commun sur la clôture algébrique $\bar{k}$ du corps k; soit a un tel vecteur pour φ, ψ, de sorte que

$$a\varphi = \mu a, \quad a\psi = \nu a, \quad \mu, \nu \in k.$$

Si $\mu = 1$ ou $\nu = 1$, on peut prendre $\theta = \varphi$ ou $\theta = \psi$ respectivement. Soient $\mu \neq 1$, $\nu \neq 1$. Puisque μ, ν engendrent dans le groupe multiplicatif du corps commutatif $\bar{k}$ un seul et même sous-groupe cyclique d'ordre q, on a $\mu = \nu^m$ pour un m naturel déterminé. Alors $\theta = \varphi\psi^{-m}$ est la transformation cherchée, car $\theta \neq 1$ et $a\theta = a$.

6.2. Entrelacements. Soient A, B deux groupes. Désignons par Fun (B, A), fun (B, A) le produit cartésien et le produit direct des copies isomorphes du groupe A indiciées par les éléments de B. Ainsi donc, Fun (B, A) est le groupe de toutes les fonctions $B \to A$ muni de l'opération de multiplication ordinaire, tandis que fun (B, A) est le sous-groupe des fonctions à supports finis. Pour $f \in$ Fun (B, A), $b \in B$, définissons une fonction f^b en posant

$$f^b(x) = f(bx), \quad x \in B. \tag{5}$$

On vérifie immédiatement que l'application

$$\hat{b}: \text{Fun}(B, A) \to \text{Fun}(B, A) \tag{6}$$

régie par la loi $f \mapsto f^b$ est un automorphisme de Fun (B, A) qui renvoie fun (B, A) sur lui-même, et que les applications

$$B \to \mathrm{Aut}\,(\mathrm{Fun}\,(B, A)), \quad B \to \mathrm{Aut}\,(\mathrm{fun}\,(B, A)), \tag{7}$$

qui font correspondre à chaque b de B l'automorphisme $\hat{b}$ et sa restriction à fun (B, A), sont des homomorphismes injectifs pour $A \neq 1$. Les extensions des groupes Fun (B, A), fun (B, A) par les groupes d'opérateurs (7) s'appellent *entrelacement cartésien* et *entrelacement direct du groupe A avec le groupe B* et se notent $A \bar{\wr} B$ et $A \wr B$ respectivement. Ainsi donc, l'entrelacement cartésien $A \bar{\wr} B$ est l'ensemble $B \cdot \mathrm{Fun}\,(B, A)$ muni de la multiplication

$$bf \cdot b'f' = bb'f^{b'}f', \text{ où } f^b\,(x) = f\,(bx), \tag{8}$$

et l'entrelacement direct $A \wr B$ est son sous-groupe $B \cdot \mathrm{fun}\,(B, A)$. Nous voyons que les groupes A et B jouent des rôles différents dans leur entrelacement : A est *passif* et B *actif*. Nous les appellerons désormais ainsi.

Les sous-groupes Fun (B, A), fun (B, A) s'appellent *fondations* ou *bases* des entrelacements correspondants. Il est évident que l'entrelacement cartésien $A \bar{\wr} B$ et l'entrelacement direct $A \wr B$ se confondent si et seulement si A est trivial ou B est fini. Le sous-groupe

$$\mathrm{Diag}\,(B, A) = \{f \mid f \in \mathrm{Fun}\,(B, A),\ f\,(x) = \mathrm{Cte} \text{ pour } x \in B\},$$

i.e. la diagonale de la base Fun (B, A), s'appelle aussi *diagonale de l'entrelacement cartésien $A \bar{\wr} B$*. Enfin, définissons pour tout $a \in A$ une fonction $\dot{a}$ de Fun (B, A) telle que

$$\dot{a}\,(x) = \begin{cases} a & \text{pour } x = e, \\ e & \text{pour } x \neq e. \end{cases}$$

On vérifie immédiatement que l'application $A \to \mathrm{Fun}\,(B, A)$ régie par la loi $a \mapsto \dot{a}$ est homomorphisme injectif. Le sous-groupe $\dot{A}$ qui correspond à A par cette application s'appelle *première copie*, et son sous-groupe conjugué $\dot{A}^b$, $b \in B$, *b-ième copie* du groupe passif. Ainsi donc, le groupe passif A intervient dans les entrelacements $A \bar{\wr} B$, $A \wr B$ par ses copies $\dot{A}^b$, tandis que le groupe actif B intervient directement dans ces entrelacements et entrelace (permute) les copies du groupe passif par conjugaisons. De toute évidence

$$\mathrm{fun}\,(B, A) = \prod_{b \in B} \dot{A}^b.$$

6.2.1. Exercice. Si $A' \leqslant A$, $B' \leqslant B$, l'entrelacement $A' \wr B'$ est isomorphe au sous-groupe de l'entrelacement $A \wr B$ engendré par

l'image du sous-groupe A' par l'injection canonique dans la première copie du groupe passif, ainsi que par le sous-groupe B'.

6.2.2. Exercice. Un sous-groupe normal non trivial d'un entrelacement direct admet une intersection non triviale avec la base (à condition, bien sûr, que le groupe passif soit non trivial).

6.2.3. Exercice. Soit A un groupe non trivial. Alors

$$Z(A\bar{\wr}B) = \mathrm{Diag}(B, Z(A)),$$
$$Z(A\wr B) = 1 \text{ si } B \text{ est infini.}$$

6.2.4. Exercice. Le commutant de l'entrelacement $A\wr B$ se confond avec le produit $[B, B]\cdot H$, où

$$H = \{f \in \mathrm{fun}(B, A) \mid \prod_{b\in B} f(b) \equiv e \pmod{[A, A]}\}.$$

6.2.5. Exercice. Chaque élément du commutant de l'entrelacement $\mathbb{Z}\wr\mathbb{Z}$ est un commutateur.

6.2.6. Exercice. L'entrelacement $\mathbb{Z}\wr\mathbb{Z}$ est isomorphe au sous-groupe engendré dans $\mathrm{GL}_n(\mathbb{R})$ par les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix},$$

où ζ est un nombre réel transcendant.

6.2.7. Exercice. Les opérations $\bar{\wr}$, $\wr$ sont non associatives dans la classe des groupes (et même dans la classe des groupes finis).

Un lien fort important entre les entrelacements et des extensions arbitraires est établi par le

6.2.8. Théorème (Kaloujnine-Krasner). *Pour toute extension d'un groupe A par un groupe B il existe un homomorphisme injectif dans l'entrelacement cartésien $A\bar{\wr}B$* (injection de Frobenius).

Démonstration. Soient $A \trianglelefteq G$, $G/A = B$, $s: B \to G$ une fonction de choix des représentants dans les classes suivant A. Soit $W = A\bar{\wr}B$. Définissons une application $\varphi_s: G \to W$ en posant $g^{\varphi_s} = \bar{g}f_g$, $g \in G$, où $\bar{g}$ est la classe Ag et f_g est un élément de la base de l'entrelacement W, défini par la formule

$$f_g(b) = ((gb)^s)^{-1}\, gb^s, \quad b \in B.$$

On vérifie immédiatement que φ_s est un homomorphisme injectif. Il s'appelle *injection de Frobenius.*

6.2.9. Exercice. Avec les mêmes notations

$$G^{\varphi_s}\cdot \mathrm{Fun}(B, A) = W, \quad G^{\varphi_s} \cap \mathrm{Fun}(B, A) = A^{\varphi_s}.$$

6.2.10. Exercice. Si s' est une autre fonction de choix, les sous-groupes G^{φ_s}, $G^{\varphi_{s'}}$ sont conjugués dans W.

Remarquons que l'entrelacement cartésien $A \bar{\wr} B$ s'appelle aussi *produit complet* ou *couronne complète* et se note A Wr B (de l'anglais *wreath product* = « produit en couronne »), tandis que l'entrelacement direct $A \wr B$ s'appelle aussi *entrelacement discret*, *produit discret* ou *couronne discrète* et se note A wr B. Au lieu de groupe passif, groupe actif on dit quelquefois *groupe inférieur*, *groupe supérieur*. Dans le § 12, nous généraliserons quelque peu la notion d'entrelacement en étudiant les représentations monomiales, le type le plus ancien des entrelacements connus. A cette même occasion nous indiquerons un plongement d'un groupe arbitraire G, contenant un sous-groupe donné H d'indice donné m, dans un groupe monomial de matrices d'ordre m sur H, qui représente la variante initiale du théorème que nous venons de démontrer.

CHAPITRE 3

GROUPES ABÉLIENS

Pour les groupes abéliens la notation additive est plus commode et plus usitée. Ce chapitre sera rédigé donc en notation additive.

§ 7. Groupes abéliens libres. Dimension

7.1. Groupes abéliens libres. Soit $\mathfrak{L}$ une classe de groupes. On dit que le groupe $F = (x_i \mid i \in I)$ de $\mathfrak{L}$ est un *groupe libre dans la classe* $\mathfrak{L}$ *à ensemble générateur libre* $\{x_i \mid i \in I\}$ si pour tout groupe $G \in \mathfrak{L}$ engendré par $\{a_i \mid i \in I\}$ l'application $x_i \to a_i$ se laisse prolonger en un homomorphisme $F \to G$. Le cardinal de l'ensemble I est appelé *degré* (*de liberté*) du groupe libre F. L'ensemble $\{x_i \mid i \in I\}$ lui-même s'appelle *base* de F. On montre que toute classe de groupes n'admet pas de groupes libres. Or, dans la classe des groupes abéliens on trouve toujours des groupes libres qui se laissent décrire sans peine.

7.1.1. Lemme. *Supposons qu'un groupe quotient G/N d'un groupe abélien G se décompose en somme directe de groupes cycliques infinis*:

$$G/N = \sum_{i \in I} (A_i/N), \quad A_i = \mathrm{gr}\,(a_i,\ N).$$

Alors G est la somme directe des sous-groupes N et $A = \mathrm{gr}\,(a_i \mid i \in I)$.

Démonstration. Remarquons d'abord que $G = \mathrm{gr}\,(N,\ A)$. Posons ensuite $A \cap N \neq 0$.

Choisissons dans l'intersection $A \cap N$ un élément non nul a qui se laisse mettre sous la forme

$$a = \sum n_k a_{i_k}.$$

Nous obtenons alors dans le groupe quotient G/N l'égalité

$$N = \sum n_k a_{i_k} + N_z$$

d'où, conformément à la définition d'une somme directe,

$$n_k a_{i_k} + N = N.$$

Puisque A_{i_k}/N est un groupe cyclique infini, l'égalité $n_k a_{i_k} + N = N$ entraîne $n_k = 0$. Ainsi donc, l'élément $a = \sum n_k a_{i_k}$ est nul, ce qui contredit l'hypothèse.

7.1.2. Théorème. *Dans la classe des groupes abéliens, seules les sommes directes de groupes cycliques infinis sont des groupes libres.*

Démonstration. Soient une somme directe $G = \sum_{i \in I} (x_i)$ de groupes cycliques infinis (x_i) et un groupe abélien quelconque A engendré par les éléments a_i, $i \in I$. Il est facile de voir que l'application $\sum n_k x_{i_k} \mapsto \sum n_k a_{i_k}$, qui prolonge l'application $x_i \mapsto a_i$ de l'ensemble $\{x_i \mid i \in I\}$ dans l'ensemble $\{a_i \mid i \in I\}$, est un homomorphisme $G \to A$. Or, cela revient à dire que G est un groupe abélien libre, i.e. un groupe libre dans la classe des groupes abéliens. Son degré de liberté est égal au nombre des sommants directs.

Soient maintenant F un groupe abélien libre et $\{x_i \mid i \in I\}$ l'ensemble de ses générateurs libres. D'après la définition d'un groupe libre, il existe un homomorphisme τ de F sur la somme directe $A = \sum_{i \in I} (a_i)$ des groupes cycliques infinis (a_i), qui prolonge l'application $x_i \mapsto a_i$. D'autre part, on vient de montrer qu'il existe un homomorphisme $\sigma: A \to F$ qui prolonge l'application $a_i \mapsto x_i$. Puisque $\tau\sigma$ laisse invariants tous les éléments générateurs du groupe F, on a $\tau\sigma = 1$ et $F \simeq A$. Le théorème est démontré.

Il se trouve que les sous-groupes d'un groupe abélien libre sont encore des groupes abéliens libres. Pour le démontrer, nous introduirons la notion de *matriochka transfinie croissante*

$$0 = N_0 < N_1 < \ldots < N_\alpha < \ldots < N_\gamma = G \qquad (1)$$

dans un groupe abélien G: c'est une suite totalement ordonnée par croissance de sous-groupes indiciés par des ordinaux transfinis. On suppose que pour un ordinal transfini limite α le sous-groupe correspondant N_α se confond avec la réunion de tous les sous-groupes N_β, $\beta < \alpha$.

Si $A \leqslant G$, le système de sous-groupes

$$0 = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_\alpha \leqslant \ldots \leqslant A_\gamma = A, \qquad (2)$$

où $A_\alpha = A \cap N_\alpha$, peut présenter des sous-groupes qui coïncident. Supprimons les termes répétitifs et numérotons à nouveau les termes de (2) par des ordinaux transfinis: nous obtenons une matriochka croissante

$$0 = A'_0 < A'_1 < \ldots < A'_\rho < \ldots < A'_\tau = A \qquad (3)$$

du sous-groupe A ; on dit qu'elle résulte de l'intersection de la matriochka (1) et du sous-groupe A.

Pour démontrer le théorème des sous-groupes, nous avons besoin d'un critère de la liberté d'un groupe commutatf.

7.1.3. Théorème. *Un groupe abélien G est libre si et seulement s'il admet une matriochka transfinie croissante dont chaque section est isomorphe au groupe cyclique infini $\mathbb{Z}$.*

Démonstration. Supposons que G admette une matriochka croissante (1) aux sections cycliques infinies. Pour tout $\alpha < \gamma$, dans la différence $N_{\alpha+1} \setminus N_\alpha$, choisissons un élément $a_{\alpha+1}$ tel que $N_{\alpha+1} = (a_{\alpha+1} + N_\alpha)$ et montrons que G se décompose en somme directe $\sum_{\alpha<\gamma} (a_{\alpha+1})$ de sous-groupes cycliques infinis $(a_{\alpha+1})$. Nous le ferons par récurrence sur la longueur γ de la matriochka (1). Pour $\gamma = 1$ l'assertion est évidente; supposons qu'il en soit ainsi pour tout $\alpha < \gamma$.

Choisissons dans le groupe G un élément quelconque $g \neq 0$ et posons $g \in N_\beta$, $g \notin \sum_{\sigma<\beta} N_\sigma = N_{\beta-1}$. En vertu de l'égalité $N_\beta = (a_\beta, N_{\beta-1})$ et du lemme 7.1.1, l'élément g se laisse mettre d'une façon unique sous la forme $g = g_1 + na_\beta$, $g_1 \in N_{\beta-1}$. Puisque $\beta - 1 < \gamma$, l'élément g_1 s'écrit d'une façon unique, par récurrence, en fonction de a_{β_i}:

$$g_1 = n_1 a_{\beta_1} + \ldots + n_s a_{\beta_s}, \quad \beta_i < \beta,$$

ce qui fait que g s'écrit, lui aussi, d'une façon unique:

$$g = n_1 a_{\beta_1} + \ldots + n_s a_{\beta_s} + na_\beta.$$

Nous venons de montrer donc que le groupe G se laisse décomposer en somme directe de sous-groupes cycliques infinis; or, en vertu du théorème 7.1.2, cela revient à dire que G est libre.

Supposons maintenant que G soit un groupe abélien libre et $G = \sum_{\alpha<\gamma} (g_\alpha)$ une décomposition de G en somme directe de sous-groupes cycliques infinis. Posant $N_0 = 0$, $N_{\alpha+1} = (g_\alpha, N_\alpha)$ et $N_\alpha = \sum_{\beta<\alpha} N_\beta$ pour un ordinal transfini limite α, nous obtenons une matriochka transfinie croissante à sections cycliques infinies. La condition est donc nécessaire. Le théorème est démontré.

Nous avons vu dans le n° 4.4 que les sections d'une matriochka sous-normale d'un sous-groupe $A \leqslant G$, obtenue en faisant l'intersection de A avec les termes d'une matriochka sous-normale de G, sont isomorphes aux sous-groupes des sections de la matriochka de G. Cette assertion se démontre d'une façon analogue pour les matriochkas transfinies croissantes (1) et (3). Le théorème 7.1.3 conduit donc

immédiatement au théorème des sous-groupes d'un groupe abélien libre :

7.1.4. Théorème. *Tout sous-groupe non nul d'un groupe abélien libre est un groupe abélien libre.*

7.1.5. Exercice. Soient n un entier positif non nul et $\mathfrak{A}_n$ la classe de tous les groupes abéliens qui vérifient l'identité $nx = 0$. Montrer que les seuls groupes libres dans $\mathfrak{A}_n$ sont les sommes directes des groupes $\mathbb{Z}_n$. Quelles sont les classes $\mathfrak{A}_n$ qui vérifient le théorème de la liberté des sous-groupes d'un groupe libre ?

7.2. Dimension d'un groupe abélien. Nous avons défini plus haut le degré d'un groupe abélien libre comme le cardinal du système de ses générateurs libres. Cette notion ne s'applique par définition qu'aux groupes abéliens libres. A présent, nous introduirons la notion de dimension d'un groupe abélien quelconque. Analogue à la notion de dimension d'un espace vectoriel, elle se confond évidemment, pour les groupes abéliens libres, avec leur degré de liberté.

Un ensemble fini d'éléments $g_1, \ldots, g_k$ d'un groupe abélien G est dit *linéairement dépendant* s'il existe des entiers relatifs non tous nuls $n_1, \ldots, n_k$ tels que $\sum n_i g_i = 0$. Un système quelconque d'éléments de G s'appelle *linéairement dépendant* si un sous-système fini de ce système est linéairement dépendant. On montre sans difficulté que dans un groupe abélien G qui contient au moins un élément d'ordre infini, il existe des systèmes d'éléments linéairement indépendants maximaux et qu'ils ont tous même cardinal. Le cardinal d'un système linéairement indépendant maximal d'éléments du groupe abélien G s'appelle *dimension*, ou plus exactement *$\mathbb{Z}$-dimension*, de ce groupe et se note $\dim G$, ou plus exactement $\dim_{\mathbb{Z}} G$.

Un groupe périodique est de toute évidence exempt de systèmes linéairement indépendants, si bien que sa dimension est nulle.

7.2.1. Théorème. *Un groupe abélien non nul sans torsion est de dimension 1 si et seulement s'il est isomorphe à un sous-groupe du groupe additif des nombres rationnels $\mathbb{Q}$.*

Démonstration. Soient $G \leqslant \mathbb{Q}$, $G \neq 0$, et g_1, g_2 deux éléments non nuls du groupe G. Il existe alors des entiers relatifs n_1, $n_2 \neq 0$ tels que $n_1 g_1 = n_2 g_2$. Ainsi donc, deux éléments non nuls quelconques de G forment un système linéairement dépendant, si bien que $\dim G = 1$.

Supposons maintenant que la dimension du groupe abélien sans torsion G soit égale à 1. Considérons un élément non nul $g_0 \in G$. Il existe alors, pour un élément quelconque $g \in G$, deux entiers relatifs n, m (non nuls si $g \neq 0$) tels que $ng = mg_0$. Puisque g est arbi-

traire, nous obtenons une relation $\varphi: g \mapsto \frac{m}{n}$ du groupe G vers le groupe $\mathbb{Q}$.

La relation φ est une application. En effet, soit encore $n_1 g = m_1 g_0$. Retranchant terme à terme l'égalité $n_1 g = m_1 g_0$ multipliée par m de l'égalité $ng = mg_0$ multipliée par m_1, on obtient $(nm_1 - n_1 m)\ g = 0$. Si $g \neq 0$, on a $nm_1 - n_1 m = 0$ et donc $\frac{m}{n} = \frac{m_1}{n_1}$. Pour $g = 0$, les deux nombres m, m_1 s'annulent,si bien que $\frac{m}{n} = \frac{m_1}{n_1} = 0$.

Soit maintenant $kg_1 = lg_0$ et $\frac{l}{k} = \frac{m}{n}$. Les égalités $ng = mg_0$, $kg_1 = lg_0$ conduisent alors à $mk\,(g - g_1) = 0$. Puisque G est sans torsion, on a $g = g_1$. L'application φ est donc injective.

Puisque des égalités $ng = mg_0$, $sg' = tg_0$, $g, g' \in G$, il ressort que $ns\,(g + g') = (sm + nd)\,g_0$, l'application φ vérifie la relation $(g + g')\,\varphi = g\varphi + g'\varphi$. Le théorème est démontré.

7.2.2. Exercice. Soit G un groupe abélien et $A \leqslant G$. On a alors $\dim G = \dim A + \dim G/A$.

7.2.3. Théorème. *Soient G un groupe abélien de dimension finie sans torsion et φ son isomorphisme sur lui-même. L'indice $|\,G : G\varphi\,|$ est alors fini.*

Démonstration. Choisissons dans G un système linéairement indépendant maximal d'éléments $a_1, \ldots, a_n$. A l'application φ on fait correspondre d'une façon naturelle une matrice $(\alpha_{ij}(\varphi))$ sur le corps $\mathbb{Q}$ en posant

$$a_i\varphi = \sum_j \alpha_{ij}(\varphi)\, a_j.$$

Plongeant G avec sa base $a_1, \ldots, a_n$ dans l'espace vectoriel $\mathbb{Q}^n$, nous pouvons prolonger φ en une transformation linéaire de $\mathbb{Q}^n$. Multiplions le polynôme caractéristique de cette transformation par le dénominateur commun de ses coefficients : soit f le polynôme sur $\mathbb{Z}$ qu'on obtient par cette opération. En vertu de la propriété fondamentale d'un polynôme caractéristique, on a $f(\varphi) = 0$, et puisque $\det \varphi \neq 0$, on a $f(0) = m \neq 0$. Alors $mG \leqslant G\varphi$. Puisque $|\,G : mG\,| \leqslant m^{\dim G} < \infty$, on a de même $|\,G : G\varphi\,| < \infty$. La proposition est démontrée.

Le lecteur prendra bien garde que tous les théorèmes bien connus de l'algèbre linéaire ne restent pas valables, loin s'en faut, pour les groupes abéliens et leurs dimensions. Par exemple, on sait bien que tout espace vectoriel se laisse décomposer en somme directe de sous-espaces de dimension 1 ; il est naturel de se demander si tout

groupe abélien sans torsion se décompose en somme directe de groupes de dimension 1. La réponse est négative:

7.2.4. Exemple (L. S. Pontriaguine). Il existe un groupe abélien G sans torsion de dimension 2 qui ne se décompose pas en somme directe $A \oplus B$, où A, B sont deux sommants de dimension 1. Nous définirons le groupe G comme un sous-groupe du groupe additif H de toutes les formes linéaires $ax+by$ à coefficients rationnels a, b; de toute évidence $H \simeq \mathbb{Q} \oplus \mathbb{Q}$, si bien que $\dim H = 2$. Soit en effet

$$G = \mathrm{gr}\,(x_0, x_1, x_2, \ldots, y),$$

où

$$x_0 = x, \quad x_i = \frac{x_{i-1}+y}{2^{2i-1}}, \quad i = 1, 2, \ldots \tag{4}$$

Un calcul bien évident montre que

$$x_i = \frac{x+(1+2+2^4+\ldots+2^{(i-1)^2})\,y}{2^{i^2}}, \quad i = 1, 2, \ldots \tag{5}$$

Puisque chaque x_{i-1} se laisse exprimer par une fonction linéaire de x_i et de y à coefficients entiers (voir (4)), il en est de même pour chaque élément $g \in G$, lorsque i est suffisamment grand. De ce fait et de (5), on déduit sans peine que si $cy \in G$, $c \in \mathbb{Q}$, on a $c \in \mathbb{Z}$; retenons-le.

Pour montrer que le groupe G est indécomposable en somme directe $A \oplus B$, il suffit de montrer qu'il n'existe dans G aucun élément g non nul qui se divise à l'infini; autrement dit, on doit montrer que pour tout $g \neq 0$ il existe un entier naturel $n(g)$ tel que l'équation $n\xi = g$ n'ait de solution dans G pour aucun $n \geqslant n(g)$. En effet, si $G = A \oplus B$, la dimension de A et de B serait alors égale à 1 (compte tenu de 7.2.2. et du fait que H est sans torsion). Puisque ni A ni B ne contiennent d'élément non nul divisible à l'infini, on a d'après le théorème 7.2.1 $A \simeq B \simeq \mathbb{Z}$, d'où $G \simeq \mathbb{Z} \oplus \mathbb{Z}$, ce qui est manifestement faux.

Il ne reste donc qu'à montrer que G ne contient aucun élément non nul divisible à l'infini. Supposons qu'il existe un élément g de ce type. Puisque tous ses multiples entiers sont divisibles à l'infini, eux aussi, on peut admettre que

$$g = ax + by, \quad \text{où} \quad a, b \in \mathbb{Z}.$$

Il ressort de (5) que les formes linéaires dans G ne peuvent admettre comme coefficients n'importe quels nombres rationnels mais seulement des fractions 2-aires; aussi la divisibilité à l'infini dans G

équivaut-elle à la divisibilité à l'infini par 2. Il existe donc dans G pour tout $i = 1, 2, \ldots$ un élément

$$u_i = \frac{1}{2^{i^2}} g = \frac{ax+by}{2^{i^2}}.$$

En vertu de (5) on a $u_i - ax_i = c_i y$, où

$$c_i = \frac{1}{2^{i^2}} [b - a(1 + 2 + 2^4 + \ldots + 2^{(i-1)^2})].$$

Conformément à la remarque faite dans le premier alinéa, c_i est un nombre entier. « Affinant » la somme entre parenthèses de façon à la transformer en une progression géométrique de raison 2, nous obtenons l'évaluation

$$1 + 2 + 2^4 + \ldots + 2^{(i-1)^2} < 2^{(i-1)^2+1},$$

d'où

$$|c_i| < \frac{|a|}{2^{2(i-1)}} + \frac{|b|}{2^{i^2}}.$$

Puisque c_i sont des entiers, ils s'annulent tous à partir d'un certain i. On a alors pour ces i

$$b - a(1 + 2 + 2^4 + \ldots + 2^{(i-1)^2}) = 0,$$

ce qui est évidemment impossible.

§ 8. Groupes abéliens de type fini

Dans ce paragraphe, nous donnerons tout d'abord un énoncé plus précis au théorème des sous-groupes d'un groupe abélien libre de degré fini et, au départ de ce nouvel énoncé, nous démontrerons le théorème fondamental sur les groupes abéliens de type fini.

8.1.1. Théorème. *Soient F_n un groupe abélien libre de degré fini n et A son sous-groupe non nul. Alors A est libre et les groupes F_n, A admettent respectivement des bases $f_1, \ldots, f_n$ et $a_1, \ldots, a_k$ telles que $k \leqslant n$, $a_i = m_i f_i$, $1 \leqslant i \leqslant k$, et m_{i+1} est multiple de m_i, $1 \leqslant i \leqslant k-1$.*

Démonstration. Soient

$$F_n = (f'_1) \oplus \ldots \oplus (f'_n),$$
$$A = (a'_1) \oplus \ldots \oplus (a'_k)$$

et

$$a'_i = \sum_j m_{ij} f'_j, \quad m_{ij} \in \mathbb{Z}.$$

On a la matrice $M = (m_{ij})$. Définissons les *fransformations élémentaires* sur les lignes et les colonnes d'une matrice entière: a) permutation de deux lignes, b) addition à une ligne d'un multiple entier d'une autre ligne, c) multiplication d'une ligne par -1, ainsi que les opérations analogues effectuées sur les colonnes. Compte tenu du fait que pour deux entiers quelconques non nuls a, b on trouve deux entiers x, y tels que $ax + by = \operatorname{pgcd}(a, b)$, on arrive, en utilisant les méthodes classiques de l'algèbre linéaire (plus exactement de la théorie des λ-matrices), à mettre la matrice M, par des transformations élémentaires de ses lignes et colonnes, sous la forme

$$\begin{pmatrix} m_1 & & & & & \\ & m_2 & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & m_k & 0 \ldots 0 \end{pmatrix}, \quad \text{où} \quad m_i | m_{i+1}.$$

Il reste à remarquer que les transformations élémentaires sur les lignes équivalent à un changement de base dans A, et les transformations élémentaires sur les colonnes, à un changement de base dans F_n. Le théorème est démontré.

8.1.2. Théorème. *Tout groupe abélien de type fini G se décompose en somme directe de sous-groupes cycliques. Plus exactement, G se décompose en somme directe de groupes cycliques infinis et de groupes cycliques primaires. En outre, le nombre des sommants cycliques infinis et la famille des ordres des sommants cycliques primaires sont les mêmes pour toute décomposition de G, i.e. ce sont des invariants du groupe G.*

Démonstration. Par définition, le groupe G est isomorphe à un groupe quotient F_n/A d'un groupe abélien libre F_n de degré fini n. En vertu du théorème 8.1.1, il existe dans F_n et A des bases $f_1, \ldots, f_n$ et $a_1, \ldots, a_k$ telles que $a_i = m_i f_i$, $1 \leqslant i \leqslant k$. Montrons que F_n/A est une somme directe de sous-groupes cycliques $(f_i + A)$.

Tout d'abord, il est clair que ces sous-groupes engendrent F_n/A. Supposons ensuite que le zéro du groupe quotient F_n/A soit de la forme

$$A = l_1 f_1 + \ldots + l_n f_n + A.$$

Alors $l_1 f_1 + \ldots + l_n f_n = a \in A$. D'autre part, exprimant l'élément a en fonction de la base $a_1, \ldots, a_k$ du sous-groupe A et tenant compte des égalités $a_i = m_i f_i$, nous aboutissons aux relations

$$l_1 f_1 + \ldots + l_n f_n = s_1 a_1 + \ldots + s_k a_k = s_1 m_1 f_1 + \ldots + s_k m_k f_k.$$

Puisque les éléments se définissent de façon unique en fonction de leurs générateurs libres f_i, on obtient $l_i = s_i m_i$, $1 \leqslant i \leqslant k$, $l_j = 0$, $k < j \leqslant n$. Or, cela veut dire que chacun des éléments $l_i f_i$ appartient à A. Le zéro se représente donc bien de façon unique sous la forme d'une somme d'éléments de sous-groupes $(f_i + A)$, si bien que le groupe G se décompose en somme directe de sous-groupes cycliques. Enfin, en vertu des résultats obtenus dans l'exercice 1.2.12, tout sous-groupe cyclique fini se laisse décomposer en somme directe de termes cycliques primaires.

Montrons maintenant que les quantités mentionnées dans le théorème sont bien des invariants. Considérons une décomposition quelconque de G en somme directe de termes cycliques infinis et de termes cycliques primaires et désignons par G_∞ et G_p les sommes directes des termes cycliques infinis et des p-termes cycliques respectivement de cette décomposition (p premier). Il est clair que G_p est un p-sous-groupe maximal et que $T = \sum_p G_p$ est un sous-groupe périodique maximal de G, si bien que le sous-groupe $G_\infty \simeq G/T$ et tous les G_p sont indépendants de la décomposition choisie. Puisque le nombre des sommants cycliques infinis est égal à $\dim G_\infty$, il est un invariant de G. Ensuite, le nombre des sommants cycliques dans la décomposition du groupe G_p coïncide avec celui de sa couche inférieure $G_p^* = \{g \in G_p \mid pg = 0\}$, donc aussi avec la dimension de l'espace vectoriel G_p^* sur le corps commutatif de p éléments, ce qui fait que ce nombre est un invariant comme le précédent. Soit enfin

$$G_p \simeq \mathbb{Z}_{p^{m_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{m_s}};$$

posons pour fixer les idées $m_1 \geqslant \ldots \geqslant m_s$. Nous allons montrer par récurrence sur $m_1 + \ldots + m_s$ que les m_i sont indépendants de la décomposition choisie. En effet,

$$G_p/G_p^* \simeq \mathbb{Z}_{p^{m_1-1}} \oplus \ldots \oplus \mathbb{Z}_{p^{m_s-1}},$$

donc, d'après l'hypothèse de récurrence, tous les m_i non inférieurs à 2 sont des invariants de la décomposition. Puisque le nombre des m_i qui restent est la différence entre s et le nombre des m_i non inférieurs à 2, il est aussi un invariant du groupe. Le théorème est démontré.

8.1.3. Exercice. Soit F un groupe abélien libre de degré fini n à base

$$f_1, \ldots, f_n. \tag{1}$$

Définissons les *transformations élémentaires* de la base (1): ce seront les passages de (1) à l'une des bases

a) $f_1, \ldots, f_j, \ldots, f_i, \ldots, f_n$, $i < j$,

b) $f_1, \ldots, f_i + mf_j, \ldots, f_j, \ldots, f_n$, $i \neq j$,

c) $f_1, \ldots, -f_i, \ldots, f_n$.

On demande de montrer qu'il existe toujours une chaîne finie de transformations élémentaires qui permet de passer de la base (1) à n'importe quelle base donnée à l'avance dans le groupe F.

8.1.4. Exercice. L'intersection des sous-groupes d'indice fini d'un groupe abélien de type fini est nulle.

8.1.5. Exercice. L'ensemble des éléments d'ordre fini d'un groupe abélien de type fini est un sous-groupe fini.

8.1.6. Exercice. Montrer, à l'aide d'un exemple, que le théorème 8.1.1. cesse d'être valable pour les groupes abéliens libres de degré infini.

Solution. Soient $G = (a_1) \oplus (a_2) \oplus \ldots$ somme directe dénombrable de groupes cycliques infinis,

$$H = \mathrm{gr}\,(b_1, b_2, \ldots), \text{ où } b_n = na_n - a_{n-1}.$$

Supposons que G et H admettent des bases compatibles; il vient alors que le groupe quotient $G/H \simeq \mathbb{Q}$ se décomposerait, lui aussi, en somme directe de groupes cycliques, ce qui est pourtant faux.

8.1.7. Exercice. Tous les sous-groupes d'un groupe abélien de type fini sont de type fini.

8.1.8. Exercice. Si A, B sont deux groupes abéliens de type fini, le groupe additif Hom (A, B) (voir la définition dans le n° 5.1.6) est de type fini.

§ 9. Groupes abéliens complets

Un groupe G est dit *complet* ou *divisible* si pour tout entier strictement positif n et tout élément $g \in G$ l'équation $nx = g$ admet au moins une solution dans G.

9.1.1. Exemples. I. Il est évident que le groupe additif $\mathbb{Q}$ des nombres rationnels est complet.

II. Montrons que le groupe quasi cyclique $\mathbb{C}_{p^\infty}$ est complet. Nous savons que le groupe $\mathbb{C}_{p^\infty}$ est isomorphe (en notation additive) à la réunion d'une famille croissante de groupes cycliques finis

$$(a_1) < (a_2) < \ldots < (a_n) < \ldots,$$

et ceci de sorte que $pa_1 = 0$, $pa_{n+1} = a_n$, $n = 1, 2, \ldots$ Considérons l'équation $sx = g$. L'élément g est contenu dans un des sous-groupes de la suite, par exemple dans (a_n), auquel cas on a $g = la_n$. Si $s = p^k m$, $(m, p) = 1$, il existe des d_1, d_2 tels que $1 = p^n d_1 + md_2$. D'où, à l'aide des égalités $g = la_n$, $p^n a_n = 0$, nous déduisons que $g = (p^n d_1 + md_2)\, g = md_2 la_n$. Cette dernière égalité entraîne, compte tenu de la relation $p^k a_{n+k} = a_n$, l'égalité $g = mp^k\,(d_2 la_{n+k})$. Ainsi donc, l'élément $d_2 la_{n+k}$ vérifie l'équation $sx = g$.

L'importance des exemples cités tient à ce que tout groupe abélien est somme directe des groupes $\mathbb{Q}$ et $\mathbb{C}_{p^\infty}$, cf. le théorème 9.1.6, dans le texte qui suit.

9.1.2. Exercice. Montrer que les images homomorphes et les sommes directes et cartésiennes des groupes abéliens complets sont complètes.

9.1.3. Théorème. *Tout groupe abélien est isomorphe à un sous-groupe d'un groupe abélien complet.*

Démonstration. Soit F un groupe abélien libre à générateurs libres x_i, $i \in I$, tel que $G \simeq F/N$. Désignons par F^* la somme directe $\sum_{i \in I} Q_i$ des groupes Q_i isomorphes au groupe additif des nombres rationnels $\mathbb{Q}$ et choisissons un b_i quelconque non nul dans chaque Q_i. Il est évident que l'application $x_i \mapsto b_i$ se prolonge en une application isomorphe τ de F dans F^*. En vertu de l'isomorphisme τ, le groupe F peut être considéré comme un sous-groupe de F^*. Conformément au résultat obtenu dans l'exercice 9.1.2, le groupe quotient F^*/N est complet; en outre, son sous-groupe F/N est isomorphe à G.

9.1.4. Théorème. *Un sous-groupe complet A d'un groupe abélien G est toujours un sommant direct dans G.*

Démonstration. Soit B un sous-groupe maximal dans G dont l'intersection avec A est nulle (l'existence de B se démontre facilement par récurrence transfinie ou à l'aide du lemme de Zorn). Démontrons l'égalité $G = A \oplus B$.

Supposons que $G \neq A \oplus B$, et choisissons un élément $g \in G$ qui ne soit pas contenu dans la somme $A \oplus B$. Le sous-groupe cyclique (g) a une intersection non nulle avec $A \oplus B$, sinon la somme $A + B + (g)$ serait directe et le sous-groupe $B \oplus (g)$, qui contient strictement B, aurait une intersection nulle avec A, ce qui contredit la condition de choix de B. Ainsi donc, $g \notin A \oplus B$, mais un multiple ng de cet élément appartient à $A \oplus B$, le nombre n étant considéré par exemple comme le plus petit nombre positif vérifiant la condition $ng \in A \oplus B$. On peut même admettre que n soit un nombre premier; s'il n'en était pas ainsi, nous prendrions au lieu de g un élément $\frac{n}{p} g$, où p est un diviseur premier de n.

En vertu du choix de g, il existe des éléments $a \in A$, $b \in B$ tels que $ng = a + b$. Puisque le sous-groupe A est complet, il contient un élément a_1 tel que $na_1 = a$. Remplaçant a par na_1 dans l'égalité précédente, on obtient $ng_1 = b$, où $g_1 = g - a_1$. Au même titre que g, l'élément g_1 n'appartient pas au sous-groupe $A \oplus B$.

En vertu du choix du sous-groupe B, l'intersection $A \cap (g_1, B)$ est distincte de zéro. Cela revient à dire qu'un élément non nul $a' \in A$ se laisse décomposer en une somme $a' = kg_1 + b'$, $b' \in B$, $0 < k < n$. Puisque $(k, n) = 1$, il existe des l, s tels que $lk + sn = 1$ et donc $g_1 = lkg_1 + sng_1$. Puisque ng_1, $kg_1 = a' - b' \in A \oplus B$, on a $g_1 \in A \oplus B$. La contradiction démontre le théorème.

9.1.5. Exercice. La somme d'une famille quelconque de sous-groupes complets d'un groupe abélien est un sous-groupe complet.

9.1.6. Théorème. *Tout groupe abélien complet non nul G se décompose en somme directe de sous-groupes isomorphes au groupe additif $\mathbb{Q}$ des nombres rationnels ou à des groupes quasi cycliques $\mathbb{C}_{p^\infty}$, avec peut-être des p premiers différents.*

Démonstration. Construisons la décomposition indiquée de G par récurrence transfinie.

Choisissons dans G un élément arbitraire non nul g. On peut le faire de deux façons:

1° L'élément g est d'ordre infini. Puisque G est complet, il existe une suite d'éléments

$$g = g_1, g_2, \ldots, g_n, \ldots$$

telle que $(n + 1)\, g_{n+1} = g_n$, $n = 1, 2, \ldots$ On vérifie facilement que le sous-groupe engendré par $g_1, g_2, \ldots$ est isomorphe au groupe additif des nombres rationnels $\mathbb{Q}$.

2° L'élément g est d'ordre fini n. Alors l'élément $a_1 = \frac{n}{p} g$, où p est un diviseur premier de n, est d'ordre premier p. Puisque G est complet, il existe comme précédemment une suite d'éléments $a_1, a_2, \ldots, pa_{n+1} = a_n$ qui engendre cette fois-ci un groupe isomorphe à $\mathbb{C}_{p^\infty}$.

Quel que soit l'ordre de g, le groupe G contient donc un sous-groupe A_1 isomorphe à $\mathbb{Q}$ ou à $\mathbb{C}_{p^\infty}$.

Supposons construite une suite de sous-groupes complets $A_1 < A_2 < \ldots < A_\beta < \ldots$, $\beta < \alpha$, telle que pour un β transfini limite il y ait $A_\beta = \sum_{\delta<\beta} A_\delta$ et pour un β transfini non limite A_β se décompose en somme directe de $A_{\beta-1}$ et d'un sous-groupe $G_{\beta-1}$ isomorphe à $\mathbb{Q}$ ou à un $\mathbb{C}_{p^\infty}$.

Si α est un ordinal limite, posons $A_\alpha = \sum_{\beta<\alpha} A_\beta$. Si α est non limite, le sous-groupe $A_{\alpha-1}$ est complet. Pour $A_{\alpha-1} \neq G$ on a en vertu du théorème 9.1.4. une décomposition directe $G = A_{\alpha-1} \oplus C$. Par analogie à la construction de A_1, choisissons dans le groupe

complet C un sous-groupe $C_{\alpha-1}$ isomorphe à $\mathbb{Q}$ ou à $\mathbb{C}_{p^\infty}$ et mettons $A_\alpha = A_{\alpha-1} \oplus C_{\alpha-1}$.

La construction par récurrence de A_α prendra fin pour un γ tel que $A_\gamma = G$.

Après avoir construit A_α, $\alpha \leqslant \gamma$, remarquons que G se décompose en somme directe de sous-groupes $A_1 = C_0, C_1, \ldots, C_\alpha, \ldots$ Le théorème est démontré.

9.1.7. Exercice. Dans un groupe abélien sans torsion, l'intersection d'une famille quelconque de sous-groupes complets est un sous-groupe complet.

9.1.8. Exercice. On appelle *complété* du groupe donné G le plus petit groupe complet G^* contenant G. Autrement dit, le complété G^* du groupe G est un groupe complet contenant G et tel que tout groupe complet A vérifiant la condition $G \leqslant A \leqslant G^*$ se confond avec G^*. Démontrer qu'un groupe abélien G sans torsion admet des complétés abéliens sans torsion. Ces complétés de G sont liés deux à deux par un isomorphisme qui prolonge n'importe quel automorphisme de G donné à l'avance.

9.1.9. Exercice. Montrer à l'aide d'un exemple que l'intersection de sous-groupes complets d'un groupe périodique n'est pas forcément un sous-groupe complet.

9.1.10. Exercice. Un groupe qui ne contient aucun sous-groupe complet non nul s'appelle *réduit*. Tout groupe abélien se décompose en somme directe d'un sous-groupe complet et d'un sous-groupe réduit.

9.1.11. Exercice. En théorie des modules, on introduit les notions très importantes de module projectif et de module injectif. Pour les groupes abéliens (qui sont des modules sur l'anneau des entiers relatifs) ces notions se définissent comme suit. On dit qu'un groupe abélien F est *projectif* (*$\mathbb{Z}$-module projectif*) si pour tout homomorphisme surjectif τ: $A \to B$ d'un groupe A sur un groupe B et pour tout homomorphisme injectif φ: $F \to B$ de F dans B il existe un homomorphisme ψ: $F \to A$ tel que le diagramme

$$\begin{tikzcd} & F \arrow[dl, dashed, "\psi"'] \arrow[d, "\varphi"] \\ A \arrow[r, "\tau"'] & B \end{tikzcd}$$

soit commutatif, i.e. $\varphi = \psi\tau$. Un groupe abélien B s'appelle *injectif* si pour tout isomorphisme τ de B sur A et tout homomorphisme

injectif φ de B dans G il existe un homomorphisme $\psi: A \to G$ tel que le diagramme

$$\begin{tikzcd} & G \\ A \arrow[ur, dashed, "\psi"] & B \arrow[l, "\tau"] \arrow[u, "\varphi"'] \end{tikzcd}$$

soit commutatif, i.e. $\varphi = \tau\psi$. On demande de montrer que

1° un groupe abélien est projectif si et seulement s'il est libre,

2° un groupe abélien est injectif si et seulement s'il est complet.

§ 10. Groupes abéliens périodiques

Dans tout groupe abélien G, l'ensemble T de ses éléments d'ordre fini forme un sous-groupe qu'on appelle parfois *partie périodique* de G. Le groupe quotient G/T est déjà apériodique (sans torsion). Grâce à ce fait, l'étude des groupes abéliens en général se trouve réduit, dans une certaine mesure, à l'étude des groupes périodiques et apériodiques. Il est à noter que la partie périodique ne constitue pas un sommant direct en général.

10.1.1. Exemple. Soit

$$\bar{G} = \sum_p \mathbf{Z}_p, \quad G = \sum_p \mathbf{Z}_p$$

(la sommation étant effectuée pour tous les p premiers). Il est évident que G est la partie périodique de $\bar{G}$. Montrons que $\bar{G}/G$ est un groupe complet et que G n'est pas un sommant direct dans $\bar{G}$.

Montrons d'abord que le groupe quotient $\bar{G}/G$ est complet. Soient $f \in \bar{G}$ et n un entier strictement positif. Puisque pour $p > n$ le groupe $\mathbf{Z}_p$ contient un élément g_p tel que $ng_p = f(p)$, on a $ng = f'$, où

$$g(p) = \begin{cases} 0 & \text{pour } p \leqslant n, \\ g_p & \text{pour } p > n, \end{cases} \quad f'(p) = \begin{cases} 0 & \text{pour } p \leqslant n, \\ f(p) & \text{pour } p > n. \end{cases}$$

Or, $fG = f'G$, aussi l'équation $nx = fG$ admet-elle une solution dans $\bar{G}/G$.

Supposons maintenant que $\bar{G}$ se décompose en somme directe $\bar{G} = G \oplus H$. Puisque $H \simeq \bar{G}/G$, il ressort de ce qui précède que le sous-groupe H est complet. Ainsi donc, l'équation $nx = h$, $h \in H$, doit avoir une solution dans H pour n quelconque. Or, si l'on a par

exemple $h(p) \neq 0$, l'équation indiquée n'admet aucune solution pour $n = p$. La contradiction obtenue confirme la conjecture sur $\overline{G}$.

Dans un groupe abélien périodique G, l'ensemble G_p de ses p-éléments, i.e. des éléments dont les ordres sont des puissances d'un p premier choisi une fois pour toutes, forme un sous-groupe. Il est évident que G_p est un p-sous-groupe maximal dans G ; il s'appelle aussi *composante primaire* dans G.

10.1.2. Exercice. Tout groupe abélien périodique se décompose en somme directe de ses composantes primaires.

Conformément à l'exercice 10.1.2, en étudiant les groupes abéliens périodiques, on peut se borner à considérer des p-groupes, au moins s'il s'agit de la décomposition du groupe. Nous nous bornerons donc, dans ce paragraphe, à formuler et à démontrer quelques propositions relatives aux p-groupes, bien qu'on puisse sans difficulté aucune les généraliser pour les groupes périodiques.

En liaison avec le théorème de décomposition d'un groupe abélien de type fini en somme directe de sous-groupes cycliques, il est naturel de se demander si cette décomposition reste valable pour un p-groupe abélien quelconque qui n'admet aucun sous-groupe complet. La réponse est négative dans le cas général ; il existe cependant quelques critères utiles qui, s'ils sont satisfaits, font que le p-groupe abélien se décompose en somme directe de sous-groupes cycliques.

10.1.3. Exemple. Soit $G = \sum_n (a_n)$ somme directe de sous-groupes cycliques (a_n) d'ordres $|a_n| = p^n$, $n = 1, 2, \ldots$, et $b_n = p^{n-1}a_n$. Posons $N = \mathrm{gr}\,(c_1, \ldots, c_n, \ldots)$, où $c_n = b_n - b_{n+1}$, et montrons que le groupe $\overline{G} = G/N$ ne contient aucun sous-groupe complet non trivial et ne se décompose pas en somme directe de sous-groupes cycliques.

En effet, le groupe quotient $\overline{G}/\overline{N}_1$ par un sous-groupe fini $\overline{N}_1$, où $\overline{N}_1 = N_1/N$, $N_1 = (b_1, N)$, se décompose en somme directe de sous-groupes cycliques $(\overline{a}_n, \overline{N}_1)/\overline{N}_1$, avec $\overline{a}_n = a_n + N$. On montre facilement que de tels groupes n'ont aucun sous-groupe complet non nul.

Puisque $b_i + N = b_{i+1} + N$, on a $p^{n-1}\overline{a}_n = \overline{a}_1$, ce qui veut dire que l'équation $p^n x = \overline{a}_1$ admet une solution dans $\overline{G}$ pour n quelconque et pour un élément $\overline{a}_1$ donné. Or, les sommes directes de p-groupes cycliques n'ont évidemment pas cette propriété. Aussi, $\overline{G}$ ne peut-il pas se décomposer en somme directe de sous-groupes cycliques.

10.1.4. Exercice. Un groupe abélien de période p première se décompose en somme directe de sous-groupes cycliques.

Indication: opérer par récurrence transfinie ou assimiler le groupe abélien de période p à un espace vectoriel sur le corps GF (p) et appliquer le théorème de l'algèbre linéaire sur la décomposition d'un espace en somme directe de sous-espaces de dimension 1.

10.1.5. Premier théorème de Prüfer. *Un p-groupe abélien de période finie se décompose en somme directe de sous-groupes cycliques.*

Démonstration. Nous allons opérer par récurrence sur la période du groupe. En vertu de l'exercice 10.1.4, nous supposons aussitôt que le théorème est valable pour les groupes de période $<p^n$ et nous considérons un groupe abélien G de période p^n.

Puisque le sous-groupe pG est de période p^{n-1}, il se décompose, d'après l'hypothèse de récurrence, en somme directe de sous-groupes cycliques, $pG = \sum_{i \in I} (a_i)$. Désignons par x_i une solution de l'équation $px = a_i$ (que cette dernière admet sûrement dans G) et posons $H = (x_i \mid i \in I)$. Remarquons que $H = \sum_{i \in I} (x_i)$. (Démontrer !)

Soit ensuite B un sous-groupe maximal dont l'intersection avec H est nulle, et soit $G \neq H + B$. Prenons un élément $g \in G$ non contenu dans $H + B$. Par construction de H, on voit que l'équation $px = pg$ admet dans H au moins une solution, par exemple h. L'élément $g_1 = g - h$ n'appartient pas à la somme $H + B$, et $pg_1 = 0$. En vertu du choix de B, l'intersection $H \cap (g_1, B) \neq 0$. Cela veut dire qu'un élément non nul $h_1 \in H$ se laisse mettre sous la forme $h_1 = kg_1 + b_1$, $b_1 \in B_1$, $0 < k < p$. D'où, si $sk \equiv 1 \pmod p$, on a $g_1 = skg_1 = sh_1 - sb_1 \in H + B$, ce qui est contraire à l'hypothèse sur g_1. On a donc $G = H \oplus B$.

Puisque H et B se décomposent chacun en somme directe de sous-groupes cycliques (le premier par construction et le second en vertu de l'exercice 10.1.4), le groupe G admet une décomposition analogue, lui aussi. Le théorème est démontré.

On dit qu'un élément $g \neq 0$ d'un p-groupe abélien G est de *hauteur finie* h dans G si l'équation $p^n x = g$ a une solution pour $n \leqslant h$ seulement. Si cette équation a une solution pour n quelconque, la hauteur de g est, par définition, infinie.

Utilisant la notion de hauteur, nous allons formuler et démontrer encore une condition suffisante de décomposition d'un p-groupe abélien en somme directe de sous-groupes cycliques. Avant de le faire, nous introduirons cependant une nouvelle notion utile, à savoir: un sous-groupe pur.

Nous disons qu'un sous-groupe A d'un groupe G est *pur* si l'équation $nx = a$ résoluble dans G pour tout n et tout élément $a \in A$ est encore résoluble dans le sous-groupe A.

10.1.6. Exercice. Dans une somme directe de groupes abéliens, chaque sommant est pur.

10.1.7. Exercice. La partie périodique d'un groupe abélien G est pure dans G.

10.1.8. Exercice. Un sous-groupe A d'un p-groupe abélien G est pur si et seulement si toute équation du type $p^n x = a$, $a \in A$, résoluble dans G l'est aussi dans A.

10.1.9. Exercice. Dans un groupe abélien G tel que $nG = 0$, un sous-groupe A est pur si et seulement si pour tout diviseur m de n et pour tout $a \in A$ l'équation $mx = a$ résoluble dans G l'est aussi dans A.

10.1.10. Exercice. Soit A un sous-groupe pur d'un groupe abélien G, qui définit dans G le groupe quotient cyclique $G/A = (g + A)$. La classe $g + A$ de G contient alors un élément g_1 tel que $|g_1| = |G/A|$.

10.1.11. Exercice. Si le groupe quotient d'un groupe abélien G par un sous-groupe pur A se décompose en somme directe de sous-groupes cycliques, A est sommant direct dans G.

Indication: utiliser l'exercice 10.1.10.

10.1.12. Théorème (Prüfer-Koulikov). *Si un sous-groupe pur A d'un groupe abélien G est de période finie, A est sommant direct dans la décomposition de G.*

Démonstration. Par hypothèse, $nA = 0$ pour un $n \neq 0$. Compte tenu du fait que A est pur, il en découle que $A \cap nG = 0$.

Montrons que le sous-groupe B/nG, où $B = A + nG$, est pur dans le groupe quotient G/nG. A cet effet, supposons que l'équation $mx = a + nG$, $a \in A$, a dans G/nG une solution $g + nG$. Conformément à l'exercice 10.1.9, on admet que m est diviseur de n, soit $n = mm_1$.

De la relation $m(g + nG) = a + nG$ découle l'égalité $mg = a + ng_1$, donc aussi $a = m(g - m_1 g_1)$. Puisque A est pur, il en résulte qu'il existe dans A un élément a_1 tel que $a = ma_1$. Or, s'il en est ainsi, l'élément $a_1 + nG$ vérifie l'équation $mx = a + nG$.

Puisque B/nG est un sous-groupe pur dans G/nG et que le groupe quotient de G/nG par B/nG se décompose en somme directe de sous-groupes cycliques en vertu du premier théorème de Prüfer, le sous-groupe B/nG est sommant direct dans G/nG conformément à 10.1.11, i.e. $G/nG = B/nG \oplus C/nG$. D'où $G = A \oplus C$, ce qu'il fallait démontrer.

10.1.13. Corollaire. *Si la partie périodique T d'un groupe abélien G est de période finie, T est sommant direct dans la décomposition de G.*

10.1.14. Deuxième théorème de Prüfer. *Un p-groupe abélien dénombrable G sans éléments de hauteur infinie se décompose en somme directe de sous-groupes cycliques.*

Démonstration. Puisque G est dénombrable, sa couche inférieure $A = \{g \in G \mid pg = 0\}$ est dénombrable, elle aussi; il existe donc dans G une suite de sous-groupes

$$0 = A_0 < A_1 < \ldots < A_n < \ldots$$

tels que $\bigcup_n A_n = A$ et $|A_{n+1} : A_n| = p$.

Soient $A_1 = (a_1)$ et b_1 solution de l'équation $p^{h_1}x = a_1$, où h_1 est la hauteur de l'élément a_1. On voit aussitôt que (b_1) est un sous-groupe pur dans G et que G se décompose donc en somme directe $G = (b_1) \oplus B_1$. Il est évident que $A_2 = A_1 + (A_2 \cap B_1)$ et que la hauteur h_2 d'un élément non nul $a_2 \in A_2 \cap B_1$ dans G se confond avec la hauteur de cet élément dans le sous-groupe B_1.

Soit $b_2 \in B_1$ solution de l'équation $p^{h_2}x = a_2$. Il existe comme précédemment une décomposition directe $B_1 = (b_2) \oplus B_2$, et ceci de telle façon que $G = (b_1) \oplus (b_2) \oplus B_2$.

Construisant de nouveaux sous-groupes (b_n) et B_n par ce procédé, on aboutit à une somme directe $C = (b_1) \oplus (b_2) \oplus \ldots$ et à une suite de sous-groupes $B_1 > B_2 > \ldots$ telles que $G = (b_1) \oplus \ldots \ldots \oplus (b_n) \oplus B_n$ et $B_2 \cap A_n = 0$.

Montrons que $G = C$. Soit $g \in G$, $|g| = p^m$. Cherchons un n tel que $p^{m-1}g \in A_n$. Soit $g = c + b$, avec $c \in (b_1) + \ldots + (b_n)$, $b \in B_n$. Puisque $p^{m-1}b \in A_n \cap B_n = 0$, on a $|b| < |g|$, ce qui revient à dire que $b \in C$. Or, on a alors aussi $g \in C$. Le théorème est démontré.

Le groupe dont il s'agit dans le deuxième théorème de Prüfer doit absolument être dénombrable, ainsi que le montre l'exemple suivant:

10.1.15. Exemple. Soient p un nombre premier, $G = \sum_n \mathbb{Z}_{p^n}$, T la partie périodique de G. Il est évident que T est un p-groupe sans éléments de hauteur infinie et a la puissance du continu. Montrons que T ne se décompose pas en somme directe de sous-groupes cycliques. A cet effet, supposons qu'au contraire $T = \sum_{i \in I} (a_i)$. Puisque T est non dénombrable, il existe une partie infinie $I_1 \subseteq I$ telle que les ordres des éléments du sous-groupe $A = \sum_{i \in I_1} (a_i)$ soient limités

dans leur ensemble, par exemple par un nombre p^k. Puisque A est sommant direct dans T, les hauteurs des éléments non nuls de A dans le groupe T ne sont jamais supérieures à k. Supposons que b_n engendre le groupe T_{p^n}. On a pour tout $f \in A$

$$f(n) \in (p^{n-k} b_n) \quad \text{pour} \quad n \geqslant k.$$

Puisque les composantes des fonctions f dans le sommant direct T_{p^n} ne parcourent qu'un ensemble fini de valeurs et que le sous-groupe A est infini, il existe dans A deux éléments distincts f_1, f_2 tels que $f_1(n) = f_2(n)$ pour $1 \leqslant n \leqslant 2k$. Leur différence $f = f_1 - f_2$ est non nulle, appartient à A et admet dans T une hauteur plus grande que k: or, cela est contraire à la construction de A.

Montrons que Iou. M. Gortchakov et Ph. Hall (voir [11]) ont établi des théorèmes absolument non triviaux analogues à ceux de Prüfer et relatifs aux groupes localement normaux.

Voyons en conclusion la structure des groupes abéliens périodiques de rang fini. Conformément à l'exercice 2.3.4, il suffit de considérer la structure des groupes primaires dont la description complète est donnée par le

10.1.16. Théorème. *Un groupe abélien primaire est de rang fini r si et seulement s'il se décompose en somme directe de r groupes quasi cycliques et groupes cycliques finis.*

Démonstration. Puisque les groupes cycliques et quasi cycliques sont de rang 1, la condition est suffisante (voir le théorème 4.1.7). Supposons ensuite que G soit un p-groupe abélien de rang fini r. Conformément à l'exercice 9.1.10, il suffit de considérer alors les deux cas suivants:

1. Le groupe G est complet. Il se décompose alors, en vertu du théorème 9.1.16, en somme directe de sous-groupes quasi cycliques. On comprend que le nombre des termes de cette somme ne peut jamais être plus grand que r.

2. Le groupe G est réduit. Montrons que G est dénombrable et ne contient aucun élément de hauteur infinie: il ne restera alors qu'à appliquer le deuxième théorème de Prüfer 10.1.14. Tout d'abord, le groupe G contient pour chaque $k = 1, 2, \ldots$ un nombre fini d'éléments qui vérifient l'équation $p^k x = 0$ (compte tenu du premier théorème de Prüfer et du rang fini de G), aussi G est-il dénombrable. Supposons ensuite que G contienne un élément non nul a de hauteur infinie; soit p^m son ordre. Choisissons dans G un élément x_k pour chaque $k = 1, 2, \ldots$, de telle façon que $p^k x_k = a$. Puisque les éléments $p^{k-1} x_k$, $k = 1, 2, \ldots$, sont tous de même ordre p^{m+1},

il existe parmi ces éléments, en vertu de ce qui précède, une sous-suite infinie d'éléments qui se confondent; désignons cet élément par a_1. De toute évidence, $pa_1 = a$ et, par construction, a_1 est de hauteur infinie, lui aussi. Poursuivant la construction par récurrence, nous obtenons des éléments $a = a_0, a_1, a_2, \ldots$ tels que $pa_{i+1} = a_i$, $i = 0, 1, 2, \ldots$; le sous-groupe qu'ils engendrent est évidemment complet, ce qui est impossible car G est réduit par hypothèse.

CHAPITRE 4

GROUPES FINIS

§ 11. Sous-groupes de Sylow

En étudiant les groupes abéliens, nous avons vu que leur structure est déterminée dans une large mesure par celle des p-sous-groupes maximaux. En théorie des groupes finis, les p-sous-groupes maximaux jouent un rôle tout aussi essentiel. Dans ce paragraphe, nous démontrerons le théorème de Sylow sur les groupes finis: pour toute puissance p^α divisant l'ordre du groupe, il existe un sous-groupe d'ordre p^α tel que si $p^{\alpha+1}$ divise l'ordre du groupe, tout sous-groupe d'ordre p^α est contenu dans un sous-groupe d'ordre $p^{\alpha+1}$; tous les p-sous-groupes maximaux sont conjugués deux à deux dans le groupe, leur nombre étant congru à 1 modulo p. Ce théorème, démontré par le mathématicien norvégien L. Sylow en 1872, fut la pierre angulaire de la théorie des groupes finis. De nombreuses généralisations de ce théorème, effectuées par des moyens différents, apparurent tant en U.R.S.S. (S. A. Tchounikhine et autres) que dans d'autres pays (Ph. Hall et autres). En liaison avec ce théorème et en l'honneur de son auteur, les p-sous-groupes maximaux des groupes finis (et souvent des groupes infinis aussi) sont appelés *p-sous-groupes de Sylow*.

Du théorème de Sylow, il ressort en particulier que tout p-sous-groupe de Sylow d'un groupe fini est exactement un sous-groupe d'ordre p^r, où p^r est la puissance maximale de p divisant l'ordre du groupe. Remarquons que si m est diviseur de l'ordre du groupe fini G sans être puissance d'un nombre premier, il se peut que G ne contienne aucun sous-groupe d'ordre m: par exemple, le groupe alterné A_4 d'ordre 12 n'a pas de sous-groupe d'ordre 6, cf. l'exercice 11.2.2.

11.1. Théorème de Sylow. Pour démontrer ce théorème, nous avons besoin de la notion d'action. On dit qu'un *groupe G opère sur un ensemble M* si pour deux éléments quelconques $m \in M$, $g \in G$ il existe un élément $mg \in M$ et que de plus $(mg_1)\, g_2 = m\,(g_1g_2)$ et $me = m$ pour tous $m \in M$, $g_1, g_2 \in G$. Ici e est l'unité du groupe G. L'ensemble $mG = \{mg \mid g \in G\}$ s'appelle *orbite* de l'élément m. Il est évident que les orbites de deux éléments quelconques de M ou

bien se confondent, ou bien ne se rencontrent pas, si bien que l'ensemble M se trouve divisé en orbites disjointes.

11.1.1. Théorème (Sylow). *Soient G un groupe fini et p un nombre premier. Existence. Pour toute puissance p^α divisant l'ordre de G, il existe un sous-groupe d'ordre p^α. Inclusion. Si $p^{\alpha+1}$ divise l'ordre de G, tout sous-groupe d'ordre p^α de G est inclus dans un sous-groupe d'ordre $p^{\alpha+1}$ de G. En particulier, tout p-sous-groupe de Sylow de G est exactement un sous-groupe d'ordre p^r, où p^r est la puissance maximale de p qui divise l'ordre de G. Conjugaison. Tous les p-sous-groupes de Sylow du groupe G sont conjugués dans G. Nombre. Le nombre des p-sous-groupes de Sylow dans G est congru à 1 modulo p et divise l'ordre de G.*

Démonstration. Existence. Soit $|G| = p^r l$, $(p, l) = 1$. Soit $\mathfrak{M}$ l'ensemble des parties de cardinal p^α dans G. Il est évident que

$$|\mathfrak{M}| = \binom{p^r l}{p^\alpha} = p^{r-\alpha} l \prod_{j=1}^{p^\alpha - 1} \frac{p^r l - j}{j},$$

aussi, la plus grande puissance de p divisant $|\mathfrak{M}|$ est-elle $p^{r-\alpha}$. Si $M \in \mathfrak{M}$, $g \in G$, il est évident que $Mg = \{mg \mid m \in M\} \in \mathfrak{M}$, si bien que G opère sur $\mathfrak{M}$ par translations à droite. Soit $\{M_1, \ldots, M_s\}$ l'orbite dont le cardinal s ne se divise pas par $p^{r-\alpha+1}$. Soit ensuite

$$G_i = \{g \mid g \in G,\ M_1 g = M_i\}, \quad 1 \leqslant i \leqslant s.$$

On vérifie immédiatement que G_1 est un sous-groupe dans G et que les G_i sont les classes à droite de G suivant G_1. Montrons que le sous-groupe G_1 est bien d'ordre p^α. Désignons provisoirement $|G_1| = t$; alors, en vertu du théorème de Lagrange 2.4.5, on a $st = |G| = p^r l$. Puisque la plus grande puissance de p divisant s est $p^{r-\alpha}$, on conçoit que p^α divise t; en particulier, $t \geqslant p^\alpha$. D'autre part, si $x \in M_1$, on a évidemment $xG_1 \subseteq M_1$, donc, $|G_1| \leqslant |M_1|$ ou $t \leqslant p^\alpha$. On a définitivement $t = p^\alpha$.

Inclusion. Soient $p^{\alpha+1}$ diviseur de $|G|$, P un sous-groupe d'ordre p^α dans G, $\mathfrak{C}$ la classe des sous-groupes conjugués de P par les éléments de G. On sait que

$$|\mathfrak{C}| = |G : N_G(P)|.$$

Si $|\mathfrak{C}|$ ne se divise pas par p, alors $|N_G(P)|$ se divise par $p^{\alpha+1}$; il existe donc dans $N_G(P)/P$, en vertu de la première proposition du théorème, un sous-groupe P^*/P d'ordre p, auquel cas P^* est le sous-groupe demandé P. Supposons maintenant que $|\mathfrak{C}|$ se divise par p.

Le groupe P opère sur $\mathfrak{C}$ par conjugaisons, et les cardinaux des orbites sont diviseurs de $|P|$, c'est pourquoi ces cardinaux se présentent sous la forme p^{α_i}, $\alpha_i \geqslant 0$. Puisqu'il existe au moins une orbite à un élément $\{P\}$ et que $|\mathfrak{C}|$ se divise par p, il existe sûrement une autre orbite à un élément $\{Q\}$. Or, cela revient à dire que P normalise Q, aussi PQ est-il un p-sous-groupe (il est à noter que $PQ/Q \simeq P/P \cap Q$ et que toute extension d'un p-sous-groupe par un p-sous-groupe est encore un p-sous-groupe). Appliquant à PQ l'automorphisme intérieur de G qui renvoie Q sur P, on obtient un p-sous-groupe $P'P$ dont P est un sous-groupe normal propre. Il existe alors comme précédemment dans $P'P/P$, toujours en vertu de la première proposition du théorème, un sous-groupe P^*/P d'ordre p, auquel cas P^* est le sous-groupe cherché.

De la proposition démontrée il ressort que tout p-sous-groupe de Sylow d'un groupe fini est exactement un sous-groupe d'ordre p^r, où p^r est la puissance maximale de p qui divise l'ordre du groupe.

Conjugaison. Soit maintenant P un sous-groupe d'ordre p^r dans G (en particulier, un p-sous-groupe de Sylow), le symbole $\mathfrak{C}$ conservant sa signification définie ci-dessus. Il s'agit de montrer que tout p-sous-groupe de Sylow Q de G est contenu dans $\mathfrak{C}$. Or, Q opère sur $\mathfrak{C}$ par conjugaisons, les orbites des éléments étant comme précédemment de cardinal p^{α_i}, $\alpha_i \geqslant 0$. Puisque maintenant $|\mathfrak{C}|$ ne se divise sûrement pas par p, il existe une orbite à un élément $\{P'\}$, i.e. Q normalise P'. Alors $P'Q$ est un p-sous-groupe et, puisque P' et Q sont maximaux, on a $Q = P'Q = P' \in \mathfrak{C}$.

Nombre. Conservant les notations de l'alinéa précédent, il suffit de vérifier que $\{Q\}$ est l'unique orbite à un élément. S'il existait une autre orbite de ce type $\{Q'\}$, alors QQ' serait un p-sous-groupe distinct de Q, ce qui est impossible. Le théorème est démontré.

Remarquons qu'au lieu d'un théorème unique, on parle parfois de trois théorèmes de Sylow: l'existence et l'inclusion font l'objet du premier, la conjugaison, du deuxième, et le nombre des p-sous-groupes de Sylow, du troisième théorème de Sylow.

11.1.2. Exercice. Un groupe d'ordre 196 contient un p-sous-groupe normal de Sylow.

11.1.3. Exercice. Les p-sous-groupes de Sylow d'un groupe infini ne sont pas toujours conjugués dans ce groupe; autrement dit, la condition de finitude dans le théorème de Sylow est essentielle.

Indication: considérer une puissance directe de S_3.

11.1.4. Exercice. Soient P un p-sous-groupe de Sylow d'un groupe fini G, et H un sous-groupe de G qui contient le normalisateur $N_G(P)$. On a alors $N_G(H) = H$.

11.2. Application aux groupes d'ordre *pq*. Le théorème de Sylow fournit souvent une information substantielle sur le groupe

fini, et si le groupe n'est pas grand — dans un sens déterminé —, il donne une description complète de ce groupe. A titre d'illustration, nous donnerons la description des groupes d'ordre pq.

Soient p, q deux nombres premiers tels que $p < q$. Quel sera le groupe G d'ordre pq? Les p- et q-sous-groupes de Sylow dans G, étant des sous-groupes d'ordre premier, sont cycliques. Soient (a), (b) des p- et q-sous-groupes de Sylow respectivement. En vertu du théorème de Sylow, le nombre des q-sous-groupes de Sylow dans G s'écrit sous la forme $1 + kq$ et divise pq, aussi le q-sous-groupe de Sylow (b) est-il unique. En particulier, (b) est normal dans G. En ce qui concerne le nombre des p-sous-groupes de Sylow, il s'écrit sous la forme $1 + kp$ et divise q. Deux cas sont alors à distinguer:

a) Le p-sous-groupe de Sylow (a) est unique. Alors (a) est normal, si bien que $[a, b] \in (a) \cap (b) = 1$. Puisque $(ab)^{pq} = a^{pq}b^{pq} = 1$, on a $G = (ab)$. On a donc dans ce cas $G \simeq \mathbb{Z}_{pq}$.

b) Il y a q p-sous-groupes de Sylow. Cela n'est certes possible qu'à condition que $q \equiv 1 \pmod p$. Soit $a^{-1}ba = b^r$. Si $r = 1$, on a comme précédemment $G = (ab)$, i.e. $G \simeq \mathbb{Z}_{pq}$. Soit $r \neq 1$. Par récurrence sur x on obtient $a^{-x}ba^x = b^{r^x}$, d'où

$$a^{-x}b^ya^x = b^{r^xy}$$

pour x, y entiers quelconques. Pour $x = p$, $y = 1$, il vient $r^p \equiv 1 \pmod q$; on obtient en outre une formule de multiplication,

$$a^xb^y \cdot a^zb^t = a^{x+z}b^{yr^z+t}. \tag{1}$$

Réciproquement, on vérifie sans peine que si $q \equiv 1 \pmod p$, $r^p \equiv 1 \pmod q$, $r \not\equiv 1 \pmod q$, cette formule de multiplication définit un groupe non abélien d'ordre pq. Enfin, les solutions de la congruence $r^p \equiv 1 \pmod q$ forment un groupe cyclique d'ordre p, aussi les solutions $\not\equiv 1 \pmod q$ se présentent-elles sous la forme $r, r^2, \ldots, r^{p-1}$, où r est une solution. Elles définissent toutes un seul et même groupe, car remplacer un générateur a par a^j revient à remplacer r par r^j.

Le théorème de Sylow aidant, nous venons donc de décrire tous les types possibles des groupes d'ordre pq: il y en a deux, un abélien et un non abélien, le second n'existant que pour $q \equiv 1 \pmod p$.

11.2.1. Exercice. Il existe seulement deux groupes non isomorphes à 6 éléments: un groupe cyclique $\mathbb{Z}_6$ et un groupe symétrique $\mathbf{S}_3$.

11.2.2. Exercice. Le groupe alterné $\mathbf{A}_4$ ne contient aucun sous-groupe d'ordre 6, bien que 6 soit diviseur de son ordre 12. La réciproque du théorème de Lagrange 2.4.5 n'est donc pas vraie, ce que nous avons signalé au commencement du paragraphe.

Solution. Si un sous-groupe à 6 éléments existait dans $\mathbf{A}_4$, il serait isomorphe à $\mathbb{Z}_6$ ou à $\mathbf{S}_3$ (exercice 11.2.1). Or, aucune permuta-

tion sur quatre symboles n'est d'ordre 6, ce qui nous amène à éliminer le premier cas. Le second est impossible lui aussi, car S_3 contient des éléments non permutables d'ordre 2 et A_4 n'en contient aucun. En effet, A_4 contient trois éléments d'ordre 2, à savoir: (12) (34), (13) (24), (14) (23), qui sont tous permutables deux à deux.

11.3. Exemples de sous-groupes de Sylow. Reprenons les groupes I à IV du chapitre 1.

11.3.1. Exemples. I. Le groupe additif de l'anneau des résidus Z_n se décompose en produit direct de ses p-sous-groupes de Sylow qui sont des sous-groupes cycliques d'ordres $p_1^{m_1}, \ldots, p_s^{m_s}$ si n admet la décomposition canonique $n = p_1^{m_1} \ldots p_s^{m_s}$.

II. Le p-sous-groupe de Sylow du groupe multiplicatif C^* est le groupe quasi cyclique C_{p^∞}.

III. Décrivons les p-sous-groupes de Sylow des groupes symétriques. Nous savons que $|S_n| = n!$ Quel est le plus grand exposant $e(n)$ pour lequel $p^{e(n)}$ est diviseur de $n!$? Dans la suite $1, 2, \ldots, n$ les multiples de p seront $p, 2p, \ldots, kp$, où $k = \left[\frac{n}{p}\right]$, donc $e(n) = \left[\frac{n}{p}\right] + e(k)$. Puisque $\left[\frac{k}{p}\right] = \left[\frac{n}{p^2}\right]$, on a $e(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$ Il est commode de décomposer n suivant la base p:

$$n = a_0 + a_1 p + \ldots + a_s p^s, \quad 0 \leqslant a_i < p, \tag{2}$$

auquel cas

$$e(n) = a_1 + a_2(1 + p) + a_3(1 + p + p^2) + \ldots$$
$$\ldots + a_s(1 + p + \ldots + p^{s-1}). \tag{3}$$

Considérons d'abord les groupes S_n, où n est une puissance de p. Supposons que S_{p^m} contienne un p-sous-groupe de Sylow, i.e. un sous-groupe H_m d'ordre $p^{1+\cdots+p^{m-1}}$: au départ de H_m, construisons dans $S_{p^{m+1}}$ un sous-groupe H_{m+1} d'ordre $p^{1+\cdots+p^m}$. A cet effet, subdivisons la suite des symboles permutables $1, 2, \ldots, p^{m+1}$ en segments successifs de longueur p^m. Si

$$c = \prod_{j=1}^{p^m} (j,\ p^m + j,\ 2p^m + j,\ \ldots,\ (p-1)p^m + j)$$

et x est une permutation sur les symboles du i-ième segment, on comprend sans peine que $c^{-1}xc$ est une permutation sur les symboles du $(i+1)$-ième segment (addition modulo p). On voit alors que le sous-groupe engendré par les sous-groupes $c^{-r}H_m c^r$, $0 \leqslant r < p$. est leur produit direct, ce qui veut dire que le sous-groupe H_{m+1} engen-

dré par le sous-groupe H_m et l'élément c est isomorphe à l'entrelacement $H_m \wr (c)$. Ici H_{m+1} est le sous-groupe cherché, car

$$| H_{m+1} | = | H_m |^p \, | c | = p^{1+\cdots+p^m}.$$

Nous remarquons en même temps que tout p-sous-groupe de Sylow dans S_{p^m} est isomorphe au groupe

$$(\ldots (\mathbb{Z}_p \wr \mathbb{Z}_p) \wr \ldots) \wr \mathbb{Z}_p$$

obtenu en faisant m fois l'entrelacement du groupe cyclique $\mathbb{Z}_p$ avec lui-même.

Soit maintenant n un nombre quelconque. Subdivisons la suite des symboles $1, \ldots, n$ en a_0 segments à un élément, a_1 segments à p éléments, etc. (voir (2)). Sur chacun des segments, considérons le groupe symétrique (qui sera d'un degré p^m) et prenons dans ce groupe un p-sous-groupe de Sylow construit comme nous venons de le décrire. Puisque ces sous-groupes opèrent sur des ensembles disjoints, le groupe P_n qu'ils engendrent est leur produit direct; son ordre est donc

$$|P_n| = \prod_{m=1}^{s} (p^{1+p+\cdots+p^{m-1}})^{a_m} = p^{\varepsilon(n)}$$

(voir (3)). Par conséquent, P_n est un p-sous-groupe de Sylow dans S_n. Il est par construction isomorphe au produit direct de quelques entrelacements successifs du type $(\ldots (\mathbb{Z}_p \wr \mathbb{Z}_p) \wr \ldots) \wr \mathbb{Z}_p$.

IV. Passons enfin aux groupes linéaires généraux sur des corps commutatifs finis. Soient p un nombre premier, m, n deux entiers $\geqslant 1$ et $q = p^m$. Montrons que $\mathbf{UT}_n(q)$ est un p-sous-groupe de Sylow du groupe $\mathbf{GL}_n(q)$. Calculons les ordres de ces groupes.

Quels n-uplets sur le corps $\mathbf{GF}(q)$ peuvent constituer la première ligne d'une matrice non dégénérée? De toute évidence, n'importe quels sauf 0; il y en a donc $q^n - 1$. La première ligne étant choisie, la deuxième peut être choisie arbitrairement, à condition qu'elle ne soit pas proportionnelle à la première; il y en a $q^n - q$. Les deux premières lignes étant choisies, la troisième peut être choisie quelconque, à condition qu'elle soit linéairement indépendante des deux premières; $q^n - q^2$ variantes sont possibles ici, et ainsi de suite. On a donc

$$|\mathbf{GL}_n(q)| = \prod_{i=0}^{n-1} (q^n - q^i). \tag{4}$$

Puisque les éléments aux angles des matrices de $\mathbf{UT}_n(q)$ parcourent le corps tout entier indépendamment les uns des autres et qu'il y a au total $\binom{n}{2}$ positions aux angles, on a $| \mathbf{UT}_n(q) | = q^{\binom{n}{2}}$. En comparant les ordres, nous voyons que $\mathbf{UT}_n(q)$ est un p-sous-groupe de Sylow dans $\mathbf{GL}_n(q)$.

11.3.2. Exercice. Ecrire les permutations qui forment un 2-sous-groupe de Sylow dans S_4.

11.3.3. Exercice. Soient p un nombre premier, m, n deux entiers naturels, $\mathbf{P}_n(\mathbb{Z}_{p^m})$ l'ensemble des matrices de $\mathbf{GL}_n(\mathbb{Z}_{p^m})$ dont les coefficients situés sous la diagonale principale sont multiples de p et les coefficients situés sur la diagonale sont congrus à 1 modulo p. Vérifier que $\mathbf{P}_n(\mathbb{Z}_{p^m})$ est un p-sous-groupe de Sylow dans $\mathbf{GL}_n(\mathbb{Z}_{p^m})$.

Indication: à l'aide de l'homomorphisme $\mathbf{GL}_n(\mathbb{Z}_{p^m}) \to \mathbf{GL}_n(\mathbb{Z}_p)$, établir la formule

$$|\mathbf{GL}_n(\mathbb{Z}_{p^m})| = \prod_{i=0}^{n-1} (p^{mn} - p^{mn-n+i}). \tag{5}$$

Formulons en conclusion quelques remarques générales sous forme d'exercices.

11.3.4. Exercice. Soit φ un homomorphisme d'un groupe fini G. Si P est un p-sous-groupe de Sylow dans G, alors P^φ est un p-sous-groupe de Sylow dans G^φ. Réciproquement, tout p-sous-groupe de Sylow dans G^φ est image d'un p-sous-groupe de Sylow dans G. Cette remarque est souvent utile quand on fait la démonstration par récurrence.

11.3.5. Exercice. Le produit de deux éléments d'ordre p peut être tant d'ordre fini, non divisible par p, que d'ordre infini. Autrement dit, l'ensemble des éléments d'ordres p^α pour p donné n'est pas toujours un sous-groupe.

11.3.6. Exercice. Soit G un groupe fini, et soit $A \leqslant G$. Si l'indice $|G : A|$ est plus petit qu'un diviseur premier p de l'ordre de G, l'intersection $\bigcap A^g$, $g \in G$, contient des p-sous-groupes de Sylow de G et, en particulier, est non triviale.

§ 12. Groupes de permutations

Nous examinerons plus en détail les groupes de permutations, qui constituent un exemple important et le premier type de groupe connu dans l'histoire. Ils furent introduits par Evariste Galois qui étudiait les conditions de résolubilité des équations algébriques par radicaux. A chaque équation algébrique il associa un groupe particulier de permutations des racines, dont la polycyclité fut une condition nécessaire et suffisante de résolubilité de l'équation par radicaux. En 1870, parut le fondamental *Traité des substitutions* ... de Camille Jordan contenant un exposé clair et détaillé des idées de Galois, ainsi que de nombreuses propriétés des permutations (ou substitutions, comme on disait à l'époque). Ce n'est que vers le début du XXe siècle que la notion moderne de groupe abstrait sortit de ces langes pour que les groupes de permutations puissent

prendre leur place modeste dans la théorie générale qu'ils occupent aujourd'hui. D'une façon générale, les groupes de permutations apparaissent tout naturellement chaque fois qu'on étudie la symétrie d'objets « de type fini »: par exemple, on associe à chaque cristal le groupe de ses rotations déterminées par les permutations de ses sommets. Une description détaillée des groupes de permutations est contenue dans le livre [41].

12.1. Représentation régulière. Il se trouve que les permutations fournissent un exemple très complet des groupes finis.

12.1.1. Théorème (Cayley). *Tout groupe fini est isomorphe à un groupe de permutations.*

Démonstration. Soit G un groupe fini qu'il s'agit de représenter par des permutations. La première question qui se pose est: par les permutations de quoi, de quel ensemble? Faute d'autre chose, prenons comme ensemble sous-jacent le groupe G lui-même. Soit g un élément de G. Quelle permutation $\hat{g}$ allons-nous lui associer? La première ligne est déjà choisie: ce sont les éléments de G numérotés de façon arbitraire. Multiplions-les à droite par g et écrivons les éléments obtenus en deuxième ligne. Des axiomes de groupe il ressort que les éléments de la deuxième ligne sont distincts deux à deux, si bien que $\hat{g}$ est en effet une permutation. Il reste à vérifier si $\hat{}$ est un isomorphisme. Or, tout d'abord $\hat{}$ est un homomorphisme, i.e.

$$\widehat{ab} = \hat{a}\hat{b} \text{ pour tous } a, b \in G.$$

En effet, les deux membres de l'égalité ont même action sur chaque élément $x \in G$:

$$x\widehat{ab} = x(ab) = (xa)b = (x\hat{a})\hat{b} = x(\hat{a}\hat{b}).$$

Ensuite, le noyau de l'application $\hat{}$ est trivial: si $\hat{g} = 1$, la permutation $\hat{g}$, d'une part, fait passer 1 en g et d'autre part laisse 1 à sa place, aussi $g = 1$. Le théorème est démontré.

12.1.2. Exercice. Tout groupe fini se plonge dans un groupe alterné.

Si l'on retire la condition de finitude de G dans la démonstration du théorème de Cayley, la même représentation par translations à droite, dite *représentation régulière* de G, conduit au

12.1.3. Théorème de Cayley généralisé. *Tout groupe est isomorphe au groupe des bijections — « permutations infinies » — d'un ensemble sur lui-même.*

La représentation des groupes abstraits par permutations s'avère utile dans les problèmes les plus divers, et non seulement en théorie des groupes finis.

12.1.4. Exemple. Sur les théorèmes de plongement. Il est souvent utile que le groupe donné G soit plongé dans un groupe plus vaste G^* caractérisé par telle ou telle propriété intéressante, par exemple:

a) G^* est un groupe simple,

b) de chaque élément de G^* on peut extraire une racine n-ième quelconque, i.e. l'équation $x^n = g$ est résoluble dans G^* pour tout élément g de G^* et tout n naturel,

c) deux éléments quelconques de G^* de même ordre, fini ou infini, sont conjugués dans G^*.

Le lecteur prolongera sans difficulté cette liste en se laissant guider par son propre goût des propriétés intéressantes.

Dans nos deux travaux communs avec V. N. Rémeslennikov (*Doklady akad. naouk SSSR*, 1960, **134**, n° 3, p. 518-520; *Outch. zap. Permskogo oun-ta*, 1960, **17**, n° 2, p. 9-11) nous avions proposé une méthode de démonstration des théorèmes de plongement: un groupe représenté à l'avance par des permutations se plonge dans un groupe de permutations qui possède déjà, dans une certaine mesure, la propriété demandée (simplicité, racines, éléments conjugants, etc.), après quoi on opère par récurrence, parfois transfinie. L'avantage de cette méthode consiste en ce que la représentation concrète du groupe abstrait par permutations concrétise les calculs et les facilite par là même. A titre d'illustration, voyons comment un groupe G se plonge dans un groupe G^* possédant la propriété c). A cet effet, construisons par récurrence la suite de groupes $G = G_0 \leqslant G_1 \leqslant \ldots$ Plus exactement, si G_n est déjà construit, nous prendrons comme G_{n+1} le groupe des transformations de l'ensemble G_n et déterminerons le plongement $G_n \leqslant G_{n+1}$ comme la représentation régulière de G_n. C'est la réunion G^* des groupes G_n qui est le groupe cherché. En effet, si a, b sont deux éléments de même ordre $r \leqslant \infty$ dans G^*, ils appartiennent à un G_n et se représentent donc dans G_{n+1} par des produits de cycles indépendants de longueur r. En accord avec l'exemple 2.5.7.III, les éléments a, b sont conjugués dans G_{n+1}, donc aussi dans G^*.

D'une façon analogue, si nous voulons plonger G dans un G^* possédant la propriété b), il suffit que G se plonge dans un groupe dans lequel l'équation $x^n = g$ soit résoluble pour n et $g \in G$ donnés. Un procédé pour obtenir ce plongement est exposé — en termes des permutations — dans les travaux mentionnés ci-dessus, ce qui résout le problème.

Enfin, le problème a) reçoit, lui aussi, une solution positive, ce que nous verrons dans le paragraphe suivant.

Une question se pose : tout groupe peut-il être plongé dans un groupe G^* qui possède les propriétés a), b), etc. en même temps ? Certes, la réponse est positive si l'on réussit à construire G^* possédant toutes ces propriétés séparément et faire en sorte que les propriétés en question restent valables sur les réunions des suites croissantes de groupes. Pour la démonstration, il suffit de répéter périodiquement les plongements des types a), b), c), ... un nombre dénombrable de fois et de passer à la réunion.

Remarquons que d'autres méthodes de démonstration des théorèmes de plongement — en particulier pour les propriétés a), b), c) définies ci-dessus — ont été proposées par Ph. Hall (*J. London Math. Soc.*, 1959, **34**, p. 305-319) et B. H. Neumann (*J. London Math. Soc.*, 1943, **18**, p. 4-11) ; la méthode de Hall utilise les entrelacements, et celle de Neumann, les produits libres avec sous-groupe amalgamé.

12.2. Représentations par permutations des classes suivant un sous-groupe. Généralisons maintenant le théorème de Cayley dans une autre direction. Soit H un sous-groupe d'indice fini dans un groupe G qui n'est pas forcément fini. A chaque élément g de G nous associons une permutation $\hat{g}$ de l'ensemble des classes à droite de G suivant H définie par analogie au n° 12.1. Notamment, si $x_1, \ldots, x_m$ sont les représentants des classes à droite de G suivant H, on pose

$$\hat{g} = \begin{pmatrix} Hx_1 & \ldots & Hx_m \\ Hx_1g & \ldots & Hx_mg \end{pmatrix}.$$

12.2.1. Théorème. *L'application ^ définie par la dernière formule est une représentation homomorphe du groupe G. Le noyau de cette représentation est le sous-groupe normal N de G qui est maximal parmi tous les sous-groupes normaux contenus dans H.*

Démonstration. Le fait que ^ soit une représentation se vérifie immédiatement sans difficulté, comme précédemment. Soit K le noyau de cette représentation. Montrons que $K \leqslant N$. Soit $g \in K$, i.e. $\hat{g} = 1$; cela veut dire que $Hxg = Hx$ pour tout $x \in G$. D'où $H^xg = H^x$ et donc

$$g \in \bigcap_{x \in G} H^x.$$

Il est clair que le second membre de cette relation est un sous-groupe normal de G contenu dans H. Il est tout aussi clair que tout autre sous-groupe de même type est contenu dans chaque H^x, aussi

$$N = \bigcap_{x \in G} H^x.$$

On a donc $g \in N$ et $K \leqslant N$. Réciproquement, $N \leqslant K$. Soit en effet $g \in N$. On a alors $Hxg = Hxgx^{-1}x = Hx$, d'où $\hat{g} = 1$ et $N \leqslant K$. Le théorème est démontré.

De ce théorème et de celui de Lagrange (n° 2.4.5) découle aussitôt le

12.2.2. Théorème (Poincaré). *Tout sous-groupe d'indice fini m contient un sous-groupe normal d'indice fini divisible par m et divisant $m!$.*

Une proposition moins forte a été déjà avancée dans le premier chapitre (voir n° 2.5.13). Le théorème 12.2.1 et le théorème 12.2.2 qui découle du précédent permettent de constater l'absence d'un sous-groupe de tel ou tel ordre dans le groupe donné (voir l'exercice 13.1.3 dans le paragraphe suivant).

12.2.3. Exercice. Un groupe de 12 éléments n'est jamais simple.

Soient R un anneau et H un groupe. On appelle *anneau de groupe* de H sur R l'anneau $R[H]$ des combinaisons linéaires formelles

$$r_1h_1 + \ldots + r_nh_n, \quad r_i \in R, \quad h_i \in H,$$

muni des lois d'addition et de multiplication:

$$\sum r_ih_i + \sum s_ih_i = \sum (r_i + s_i)\, h_i,$$
$$\sum r_ih_i \cdot \sum s_jf_j = \sum r_is_jh_if_j$$

(nous avons déjà décrit un objet de ce type page 37).

Revenons maintenant au commencement de ce n° et remarquons que la représentation $g \mapsto \hat{g}$ associe à chaque g de G une « permutation de représentants » $\pi(g)$ et des « facteurs supplémentaires » $h_i(g)$:

$$Hx_ig = Hx_{i\pi(g)}, \quad x_ig = h_i(g)\, x_{i\pi(g)}.$$

On voit immédiatement que la formule

$$g \mapsto \operatorname{diag}(h_1(g), \ldots, h_m(g)) \cdot \pi(g)$$

définit un homomorphisme injectif $G \to \mathrm{GL}_m(\mathbb{Z}[H])$, où $\mathbb{Z}[H]$ est l'anneau de groupe de H sur $\mathbb{Z}$ et la permutation $\pi(g)$ est transcrite au moyen d'une matrice composée de zéros et d'unités. Cet homomorphisme injectif s'appelle *représentation monomiale du groupe G sur le sous-groupe H*. Nous voyons que tout groupe où H est sous-groupe d'indice m se plonge dans le groupe des matrices d'ordre m sur $\mathbb{Z}[H]$, dont chaque ligne et chaque colonne contiennent un seul élément non nul de H (*sous-groupe monomial* du groupe $\mathrm{GL}_m(\mathbb{Z}[H])$).

La construction décrite est surtout employée en théorie des représentations linéaires des groupes finis où elle fournit la représentation d'un groupe induite par celle d'un sous-groupe.

Tout cela se traduit facilement dans le langage des entrelacements.

Soient A, B deux groupes, et soit $B \leqslant \mathrm{S}(X)$, où X est un ensemble. On vérifie sans peine que l'ensemble $B.\mathrm{Fun}(X, A)$ muni de la multiplication

$$bf.b'f' = bb'f^{b'}f', \quad \text{où} \quad f^b(x) = f(xb^{-1}), \quad x \in X,$$

est un groupe. Il s'appelle *entrelacement du groupe A avec le groupe des permutations B*. Le cas le plus important de cette notion a été examiné dans le chapitre 2: il s'appelle *entrelacement standard* et s'obtient en représentant B par des permutations de lui-même suivant la loi $x \mapsto b^{-1}x$. Avec les mêmes symboles d'entrelacements qu'auparavant, nous voyons que le sous-groupe monomial de $\mathrm{GL}_m(\mathbb{Z}[H])$ est exactement $H \wr \mathrm{S}_m$ et que le théorème 6.2.8 traduit la situation décrite plus haut pour les entrelacements standards.

12.3. Transitivité. Primitivité. Nous allons considérer certaines notions relatives aux groupes de permutations et liées essentiellement à leur action sur l'ensemble des symboles permutés. En réalité, ces notions s'appliquent à des groupes arbitraires opérant sur un ensemble: c'est la raison pour laquelle nous plaçons nos définitions dans un contexte plus large que nécessaire.

Si un groupe G opère sur un ensemble M avec une orbite unique — M lui-même —, on dit que G est *transitif* (sur M). Cela revient évidemment à demander que pour deux éléments quelconques m, m' de M il existe dans G un élément g tel que $mg = m'$. En généralisant, on dit que le groupe G est *r fois transitif* si pour deux r-uplets quelconques $\{m_1, \ldots, m_r\}$ et $\{m'_1, \ldots, m'_r\}$ d'éléments de M il existe dans G un élément g tel que $m_i g = m'_i$, $1 \leqslant i \leqslant r$. La partition de l'ensemble M en parties disjointes $\{M_\alpha\}$ s'appelle *partition en blocs par rapport à G* si pour toute M_α et tout $g \in G$ il existe une M_β telle que $M_\alpha g = M_\beta$, i.e. si les éléments de G permutent les parties (*blocs*) M_α tout entières. Il existe bien sûr toujours des partitions triviales: la partition en blocs à un élément et la partition qui se réduit à un bloc unique. Si M n'admet aucune partition en blocs non triviale, on dit que le groupe G est *primitif*. En particulier, toutes ces notions s'étendent aux groupes des permutations d'un ensemble fini M considérés avec leur action naturelle sur M.

12.3.1. Exercice. La condition $M_\alpha g = M_\beta$ dans la définition d'une partition en blocs est équivalente à la condition moins forte formellement $M_\alpha g \subseteq M_\beta$.

12.3.2. Exercice. Les groupes S_n, A_n sont n fois et $(n-2)$ fois transitifs respectivement.

12.3.3. Exercice. Tout groupe doublement transitif est primitif.

12.3.4. Exercice. Tout sous-groupe normal non trivial N d'un groupe primitif G est transitif.

Indication: les orbites pour N constituent un système complet de blocs pour G.

Supposons que deux groupes G, G' opèrent respectivement sur deux ensembles M, M'. Il est naturel de les appeler *isomorphes* — comme des groupes de transformations — s'il existe une bijection de M sur M' (par exemple φ) et un isomorphisme de G sur G' (par exemple ψ) par lesquels les éléments correspondants des groupes envoient les éléments correspondants des ensembles de nouveau dans des éléments qui se correspondent, i.e. si

$$m^{\varphi}g^{\psi} = (mg)^{\varphi} \quad \text{pour tous} \quad m \in M, \quad g \in G.$$

Les groupes de permutations isomorphes sont aussi appelés *groupes semblables*.

Dans le n° précédent, nous avons associé à tout sous-groupe d'indice fini une représentation homomorphe du groupe par des permutations de l'ensemble des classes suivant le sous-groupe. On voit sans peine que cette représentation est transitive. La réciproque est aussi vraie: toute représentation transitive d'un groupe donné par des permutations est semblable à une représentation décrite plus haut par des permutations des classes à droite suivant un sous-groupe d'indice fini. On a le

12.3.5. Théorème. *Soit π un homomorphisme d'un groupe G sur un groupe transitif de permutations d'un ensemble M. Supposons que G opère sur M suivant la loi $mg = mg^{\pi}$. Soient $m_1 \in M$ et H stabilisateur de m_1 dans G, i.e.*

$$H = \{g \mid g \in G,\ m_1 g = m_1\}.$$

Alors H est un sous-groupe d'indice fini dans G et le groupe G^{π} est semblable au groupe des permutations des classes de G suivant H, décrit dans le n° précédent.

Démonstration. Soit $M = \{m_1, \ldots, m_s\}$. Désignons

$$H_i = \{g \mid g \in G,\ m_1 g = m_i\}, \qquad 1 \leqslant i \leqslant s.$$

En vertu de la transitivité de G^{π}, tous les H_i sont non vides. On voit immédiatement que H_1 est un sous-groupe dans G et que les H_i sont les classes à droite de G suivant H_1. Puisque $H = H_1$, c'est un sous-groupe d'indice fini dans G.

Soit π' la représentation indiquée de G par des permutations des classes à droite de G suivant H. Il reste à montrer que les groupes de permutations G^{π} et $G^{\pi'}$ sont semblables. Soient φ une application

de M dans l'ensemble des classes à droite de G suivant H qui fait passer m_i en H_i, et ψ une application de G^π dans $G^{\pi'}$ qui fait passer g^π en $g^{\pi'}$. On vérifie aisément que pour $x^\pi = y^\pi$ on a $x^{\pi'} = y^{\pi'}$, i.e. que l'application ψ est bien définie. Maintenant on vérifie immédiatement que φ, ψ sont deux bijections et que

$$m_i^\varphi (g^\pi)^\psi = (m_i g^\pi)^\varphi \quad \text{pour} \quad 1 \leqslant i \leqslant s, \quad g \in G.$$

Le théorème est démontré.

Montrons que l'étude des groupes de permutations arbitraires se réduit dans une certaine mesure à l'étude des groupes transitifs, et l'étude de ces derniers, à celle des groupes primitifs. Rappelons qu'on entend par produit sous-direct de groupes G_i un sous-groupe de leur produit direct dont la projection sur chaque facteur G_i se confond avec G_i tout entier.

12.3.6. Théorème. *Tout groupe de permutations sur n symboles est produit sous-direct de groupes de permutations transitifs sur n_i symboles, où $\sum n_i = n$. Soit G un groupe de permutations transitif d'un ensemble M; étant donnée une partition de M en blocs minimaux M' de cardinal $\geqslant 2$, le stabilisateur d'un bloc entier M', i.e. l'ensemble*

$$H = \{g \mid g \in G,\ M'g = M'\},$$

est un sous-groupe de G opérant primitivement sur M'.

Démonstration. Soient G un groupe de permutations d'un ensemble M, M_i les orbites correspondantes, G_i le groupe des permutations de M_i induit par l'action de G sur M_i. Il est clair que G est produit sous-direct des G_i.

Démontrons à présent la deuxième proposition. Il est évident que H est un sous-groupe. Soient $x_1, \ldots, x_s$ les représentants des classes à droite de G suivant H. Alors $M'x_1, \ldots, M'x_s$ est la partition initiale de M en blocs (utiliser la transitivité de G). Si H opérait sur M' de façon non primitive, il existerait une partition non triviale de M' en blocs $M'_1, \ldots, M'_r$ par rapport à H. Or, on pourrait alors affiner la partition initiale de M par rapport à G en partition $M'_i x_j$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Le théorème est démontré.

12.3.7. Théorème. *Soit G un groupe de permutations transitif d'un ensemble M. Soit une partition de M en blocs; soient M_1 un bloc quelconque et m_1 un point de M_1. Soient H le stabilisateur de m_1 et K le stabilisateur de M_1 tout entier, i.e.*

$$H = \{g \mid g \in G,\ m_1 g = m_1\},$$
$$K = \{g \mid g \in G,\ M_1 g = M_1\}.$$

Alors H et K sont des sous-groupes de G, tels que $H \leqslant K \leqslant G$. Le nombre total des blocs est $|G:K|$ et chaque bloc se compose de $|K:H|$ éléments.

Démonstration. La première proposition est immédiate par définition. Soient ensuite $Hx_1, \ldots, Hx_s$ les classes à droite de G suivant H, avec $x_1 = 1$. En vertu du théorème 12.3.5, on suppose que $M = \{Hx_1, \ldots, Hx_s\}$ et que G opère sur M par translations à droite. Soient $M_1 = \{Hx_1, \ldots, Hx_r\}$, $m_1 = H$. Le groupe G étant transitif, chaque bloc s'obtient à partir de M_1 par une translation à droite effectuée par un élément de G: pour cette raison tous les blocs sont équipotents. Il suffit donc de vérifier que $r = |K:H|$ ou que

$$K = Hx_1 \cup \ldots \cup Hx_r.$$

Or, d'une part, chaque hx_i, $h \in H$, $1 \leqslant i \leqslant r$, fait passer la classe H en une classe de M_1, ce qui veut dire que le bloc M_1 revient tout entier à lui-même. Donc

$$Hx_1 \cup \ldots \cup Hx_r \subseteq K.$$

D'autre part, si $x \in K$, on a $Hx = Hx_i$ pour un i tel que $1 \leqslant i \leqslant r$, d'où l'inclusion inverse.

§ 13. Groupes finis simples

De même que les entiers naturels s'obtiennent à partir des nombres premiers au moyen de la multiplication, tout groupe fini se laisse obtenir par extension d'un groupe fini simple. En effet, soit dans un groupe fini G une matriochka sous-normale sans répétitions

$$1 = G_0 < G_1 < \ldots < G_m = G,$$

i.e. une matriochka dont chaque terme précédent est un sous-groupe normal propre du suivant. Si une section G_{i+1}/G_i n'est pas un groupe simple, on peut, en prenant dans cette section un sous-groupe normal propre H/G_i, subdiviser la matriochka au moyen de l'intercalation $G_i < H < G_{i+1}$: aussi une matriochka sous-normale non subdivisible sans répétitions a-t-elle toutes ses sections simples. Dans ce sens, les groupes finis simples sont des blocs dont l'assemblage conduit à un groupe fini arbitraire. La différence par rapport aux nombres consiste en ce que le résultat n'est pas défini ici par les seuls blocs choisis mais dépend encore du procédé d'assemblage. Un exemple trivial des groupes simples est donné par les groupes cycliques d'ordre premier; il est évident que c'est l'unique type des groupes simples abéliens. La classification des groupes finis simples est un problème extrêmement important, peut-être même le plus important, en théorie des groupes finis à l'heure actuelle, bien que

la théorie ne se réduise pas entièrement à ce problème. L'offensive est menée en plusieurs directions: certains chercheurs développent des méthodes générales, « industrielles », afin de mettre au point un procédé unique d'obtention des groupes finis simples (on doit ranger sous cette étiquette certains résultats assez fins d'identification des groupes obtenus par des procédés différents); d'autres au contraire, se fiant à leur intuition et espérant un coup de fortune, cherchent des exemples isolés (la valeur de chaque trouvaille, i.e. de chaque nouveau groupe simple, est aujourd'hui exceptionnelle); d'autres encore font leur classification en se donnant telle ou telle condition auxiliaire, par exemple un sous-groupe de Sylow déterminé, et ainsi de suite. Dans les années soixante le célèbre problème de Burnside, réputé inexpugnable depuis un demi-siècle, fut pris d'assaut: W. Feit et J. G. Thompson [9] montrèrent que tout groupe fini simple non cyclique contient un nombre pair d'éléments (ce théorème s'énonce cependant, le plus souvent, sans faire mention des groupes simples: *tout groupe impair*, i.e. groupe fini d'ordre impair, *est polycyclique*).

Le présent paragraphe poursuit un but modeste: indiquer deux séries classiques de groupes finis simples, à savoir les groupes alternés et les groupes linéaires spéciaux projectifs. Les démonstrations que nous allons citer sont artisanales et ne donnent aucune idée des méthodes industrielles dont nous venons de parler. Le lecteur trouvera un bon rappel des résultats actuels dans ce domaine, ainsi que la liste des groupes finis simples connus, dans l'article de M. Aschbacher [2].

13.1. Groupes alternés. Dans ce n° nous ferons usage de la remarque III de l'exemple 2.5.7.

13.1.1. Théorème (Galois). *Pour $n \neq 4$ le groupe alterné $\mathbf{A}_n$ est simple. Le groupe $\mathbf{A}_4$ est non simple.*

Démonstration. a) Les groupes $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$ sont d'ordre 1, 1 et 3 respectivement, i.e. sont simples. Le groupe $\mathbf{A}_4$ n'est pas simple: conformément à l'exemple 4.4.1.III, il admet une matriochka polycyclique à sections d'ordres 2, 2, 3. Soient maintenant $n \geqslant 5$ et N un sous-groupe normal $\neq 1$ de $\mathbf{A}_n$; il s'agit de montrer que $N = \mathbf{A}_n$. Puisque le groupe $\mathbf{A}_n$ est engendré par des cycles de trois éléments (voir l'exemple 2.2.2.III), il suffit de montrer qu'ils sont contenus tous dans N. Nous le ferons en étapes.

b) Puisque N contient une permutation paire non triviale, on peut, en la décomposant en produit de cycles indépendants, admettre que N contient une des permutations suivantes:

1° $a = (1234\ldots)\ldots$, i.e. la décomposition de a comporte un cycle de longueur $\geqslant 4$,

2° $a = (123)(45\ldots)\ldots$, i.e. la décomposition contient un cycle de trois éléments et d'autres cycles,

3° $a = (123)$,

4° $a = (12)(34)\ldots$, i.e. a est un produit de transpositions indépendantes.

c) Le sous-groupe N contient au moins un cycle de trois éléments. En effet, N contient le commutateur $[a, b] = a^{-1}(b^{-1}ab)$ pour tout $b \in A_n$. En posant

$$b = \begin{cases} (123) \text{ dans le cas } 1^\circ, \\ (124) \text{ dans le cas } 2^\circ, \\ (123) \text{ dans le cas } 4^\circ, \end{cases}$$

on obtient après un calcul bien simple

$$[a, b] = \begin{cases} (124) \text{ dans le cas } 1^\circ, \\ (12534) \text{ dans le cas } 2^\circ, \\ (13)(24) \text{ dans le cas } 4^\circ. \end{cases}$$

Le cas 2° s'en trouve réduit à 1°, lequel se réduit à son tour à 3°; or, dans le cas 3° la proposition est triviale. Il reste à considérer le cas 4°. En conjuguant la permutation $[a, b]$ par la permutation paire (12534), nous obtenons (24)(15) (voir la remarque III de l'exemple 2.5.7), puis, en multipliant $[a, b]$ par cette permutation, nous obtenons (135).

d) Le sous-groupe N contient tous les cycles de trois éléments. En effet, N contient un cycle $(i_1i_2i_3)$ en vertu de ce qui précède. Soit $(j_1j_2j_3)$ un autre cycle quelconque de trois éléments. Puisque $n \geqslant 5$, il existe une permutation paire de la forme

$$\begin{pmatrix} i_1 & i_2 & i_3 & \cdots \\ j_1 & j_2 & j_3 & \cdots \end{pmatrix}.$$

Conjuguant $(i_1i_2i_3)$ par cette permutation, on retrouve $(j_1j_2j_3)$. Le théorème est démontré.

Remarquons que les étapes a)-d) de cette démonstration constituent une voie typique et en principe universelle de démonstration de la simplicité : on choisit dans le sous-groupe normal N un élément a dont on sait seulement qu'il est distinct de l'unité, puis, sachant qu'on reste dans N en effectuant la multiplication et l'inversion, ainsi que la conjugaison et la commutation par un élément quelconque du groupe, on tire de N ses éléments un à un jusqu'à découvrir tous les générateurs du groupe. Un philosophe condescendu à discuter le théorème de Galois pourrait décréter: saisissez un anneau et vous tirerez toute la chaîne. Cette excellente idée directrice passe malheureusement sous silence les modalités de l'extraction.

13.1.2. Exercice. Si $\mathfrak{n}$ est un cardinal arbitraire, on appelle *groupe alterné de degré* $\mathfrak{n}$ le groupe $A_{\mathfrak{n}}$ des transformations d'un ensemble de cardinal $\mathfrak{n}$ dont chacune ne déplace réellement qu'un nombre fini de symboles et se décompose en produit d'un nombre pair de transpositions. Reprenant la démonstration du théorème de Galois, montrer que $A_{\mathfrak{n}}$ est simple pour $\mathfrak{n} \neq 4$.

A propos du dernier exercice, faisons une remarque. Supposons que, comme en théorie des ensembles, ω_ν désigne un $(\nu+1)$-ième cardinal infini. Soient M un ensemble de cardinal ω_ν et $S_\mu(M)$ l'ensemble des applications de $S(M)$ qui déplacent en réalité un ensemble de symboles de cardinal $<\omega_\mu$. Il est clair que la matriochka transfinie croissante

$$1 < A_{\omega_\nu} < S_0(M) < S_1(M) < \ldots < S_\nu(M) < S(M) \quad (1)$$

se compose des sous-groupes normaux de $S(M)$. Il se trouve que tout sous-groupe normal de $S(M)$ correspond à un terme de la matriochka en question (R. Baer, *Studia math.*, 1934, 5, p. 15-17). En particulier, la section $S(M)/S_\nu(M)$ est un groupe simple. Remarquons enfin qu'à la lumière de ces faits le problème 12.1.4, a) se résout tout à fait facilement. En effet, pour les groupes finis la solution est immédiate en vertu de l'exercice 12.1.2. Si le groupe G est de cardinal ω_ν infini, on fait sa représentation régulière à la suite de laquelle il se trouve plongé dans $S(G)$ où son intersection avec $S_\nu(G)$ est égale à l'unité, ce qui fait que G est injecté par un homomorphisme dans $S(G)/S_\nu(G)$.

13.1.3. Exercice. Le groupe alterné A_5 d'ordre 60 ne contient pas de sous-groupes d'ordre 15, 20, 30.

Solution. Si A_5 contenait un sous-groupe d'ordre 15, i.e. d'indice 4, il contiendrait alors, en vertu du théorème 12.2.2, un sous-groupe normal d'indice fini divisible par 4 et divisant 24. Or, cela est impossible, car A_5 est un groupe simple d'après le théorème de Galois. Les autres cas se traitent de façon analogue.

13.2. Groupes linéaires spéciaux projectifs. Soit K un corps commutatif. On appelle *groupe linéaire spécial projectif* le groupe quotient $PSL_n(K)$ du groupe linéaire spécial $SL_n(K)$ par son centre (sous-groupe de matrices scalaires). C'est C. Jordan qui a introduit ces groupes (sur les corps commutatifs finis) en 1870 (parmi d'autres séries de groupes) et montré qu'ils sont simples. Quelques erreurs dans la démonstration initiale de Jordan ont été éliminées plus tard par Dickson.

13.2.1. Exercice. Les fonctions homographiques

$$f(x) = \frac{ax+b}{cx+d}$$

à coefficients dans K, de déterminant $ad - bc = 1$, forment, par rapport à la superposition, un groupe isomorphe à $\mathrm{PSL}_2(K)$.

13.2.2. Exercice. Vérifier les formules

$$|\mathrm{SL}_n(q)| = \frac{1}{q-1} \prod_{i=0}^{n-1} (q^n - q^i), \tag{2}$$

$$|\mathrm{PSL}_n(q)| = \frac{1}{d(q-1)} \prod_{i=0}^{n-1} (q^n - q^i), \text{ où } d = (n, q-1). \tag{3}$$

Indication: assimiler SL au noyau de l'homomorphisme det et appliquer la formule (4) du § 11, puis utiliser l'exercice 3.1.6.

Pour démontrer le théorème de Jordan-Dickson sans demander que le corps commutatif soit fini, nous utiliserons la condition de simplicité suivante:

13.2.3. Lemme. *Un groupe primitif G de transformations d'un ensemble M est simple si*

1° *G se confond avec son commutant G',*

2° *le stabilisateur S_m d'un élément m de M contient un sous-groupe normal abélien A_m tel que*

$$G = \mathrm{gr}(A_m^g \mid g \in G). \tag{4}$$

Démonstration. a) Soit N un sous-groupe normal $\neq 1$ de G: il s'agit de montrer que $G = N$. Remarquons d'abord que $G = S_m N$. En effet, N est transitif en vertu de l'exercice 12.3.4, aussi pour tout $g \in G$ existe-t-il un $h \in N$ tel que $mh = mg$. On a donc $gh^{-1} \in S_m$ et $g \in S_m N$.

b) Ensuite, $G = A_m N$. En effet, tout élément g de G se laisse mettre, conformément à (4), sous la forme

$$g = a_1^{g_1} \ldots a_s^{g_s}, \quad a_i \in A_m, \quad g_i \in G,$$

et, conformément à a), on peut admettre que chaque g_i appartient à N. Comme A_m et N sont permutables, on a $g \in A_m N$.

c) Enfin, $G = N$. En effet, on a conformément à 1°, à b) et en vertu des identités pour les commutateurs indiquées dans le § 3

$$G = [A_m N, A_m N] \leqslant N.$$

Le lemme est démontré.

13.2.4. Théorème (Jordan-Dickson). *Pour tout corps commutatif K le groupe $\mathrm{PSL}_n(K)$ est toujours simple, à l'exception de deux cas: $\mathrm{PSL}_2(2)$ et $\mathrm{PSL}_2(3)$.*

Démonstration. Tout d'abord, les deux groupes indiqués sont d'ordres 6 et 12 (voir la formule (3)), ce qui signifie bien qu'ils

sont non simples (voir les exercices 11.2.1 et 12.2.3). Passant au cas général, considérons l'action naturelle d'un groupe $G = \mathbf{PSL}_n(K)$ sur l'ensemble M de toutes les droites d'un espace vectoriel de dimension n sur le corps K avec une base donnée quelconque $e_1, \ldots, e_n$ et voyons si G, M vérifient toutes les conditions du lemme 13.2.3.

Puisque deux couples quelconques de droites distinctes admettent toujours une transformation linéaire par laquelle le premier couple se réduit au second, le groupe G est doublement transitif, donc primitif (voir l'exercice 12.3.3).

Par ailleurs, G se confond avec son commutant, ce qui résulte immédiatement de la formule (8) de l'exemple 3.2.1 (c'est là qu'on élimine les deux groupes exceptionnels).

Vérifions enfin la condition 2°. Soit m une droite de vecteur directeur e_n. Il est clair que le stabilisateur S_m (ou plus exactement son image réciproque dans le groupe $\mathbf{SL}_n(K)$) se compose de toutes les matrices de la forme

$$\left(\begin{array}{c|c} & * \\ & \cdot \\ * & \cdot \\ & \cdot \\ & * \\ \hline 0 \ldots 0 & * \end{array}\right).$$

L'application de S_m sur la paire de blocs diagonaux est un homomorphisme dont le noyau A_m se compose de toutes les matrices de même forme avec des unités dans les blocs diagonaux. Il est évident que A_m est un groupe abélien ; il ne reste qu'à vérifier la formule (4). Puisque le groupe $\mathbf{SL}_n(K)$ est engendré par ses transvections $t_{ij}(\alpha)$ (voir l'exemple 2.2.2.IV), il suffit de vérifier que $t_{ij}(\alpha)$ est la conjuguée dans $\mathbf{SL}_n(K)$ d'une transvection $t_{1k}(\alpha)$. Or, si $i = 1$, la chose est triviale, et si $i \neq 1$, on peut prendre comme matrice de conjugaison la matrice de transition de la base donnée $e_1, \ldots, e_i, \ldots$ à la base $-e_i, \ldots, e_1, \ldots$, où tous les vecteurs non écrits restent inchangés. Le théorème est démontré.

13.2.5. Exercice. En liaison avec le théorème de Jordan-Dickson, il est naturel de se demander s'il est possible d'obtenir de nouveaux groupes finis simples en remplaçant dans la définition de $\mathbf{PSL}_n(K)$ le corps commutatif K par l'anneau des résidus $\mathbb{Z}_m$. Ces espérances sont sans fondement : si m est premier, nous nous retrouvons dans le cas d'un corps, et si m est non premier, le groupe $\mathbf{PSL}_n(\mathbb{Z}_m)$ est non simple.

13.2.6. Exercice. Indiquer un groupe dont le centre définit un groupe quotient simple sans être un facteur direct lui-même.

S o l u t i o n. Si le centre Z composé des matrices $\pm e$ dans le groupe $\mathbf{SL}_2(5)$ avait un supplémentaire H, une des matrices

$$\pm\begin{pmatrix} \frac{1}{\zeta} & 0 \\ 0 & \zeta \end{pmatrix}$$

serait contenue dans H, où ζ est un générateur du groupe multiplicatif du corps commutatif de 5 éléments. Or, le carré $-e$ de cette matrice appartiendrait alors à l'intersection $Z \cap H$, ce qui est impossible.

J.G. Thompson (*Pacif. J. Math.*, 1964, 14, n° 1, p. 363-364) a appelé un sous-groupe A d'un groupe fini G son 2-*signalisateur* si l'ordre $|A|$ et l'indice $|G: N_G(A)|$ sont impairs. Il a avancé l'hypothèse (ibid.) que les 2-signalisateurs des groupes finis simples sont toujours abéliens. Nous allons terminer le chapitre par un exemple qui réfute cette hypothèse: il appartient à V. D. Mazourov (*Alguebra i loguika*, 1968, 7, n° 3, p. 60-62) et est fondé uniquement sur la simplicité des groupes **PSL**.

13.2.7. E x e m p l e. Tout groupe simple $\mathbf{PSL}_7(q)$ pour q impair contient des 2-signalisateurs non abéliens. En effet, considérons dans $G = \mathbf{SL}_7(q)$ deux sous-groupes A, B composés respectivement par toutes les matrices de la forme

$$\begin{pmatrix} 1 & * & * \\ 0 & e_2 & * \\ 0 & 0 & e_4 \end{pmatrix}, \quad \begin{pmatrix} \alpha(x, y) & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & y \end{pmatrix}, \quad \alpha(x, y) = \frac{1}{\det x \cdot \det y},$$

où e_k est la matrice unité d'ordre k et la partition en blocs est la même dans les deux cas. Compte tenu de la formule (2) du présent paragraphe et de la formule (4) du § 11,

$$|G| = \frac{1}{q-1}(q^7-1)(q^7-q)\ldots(q^7-q^6), \quad |A| \text{ est une puissance de } q,$$

$$|B| = (q^2-1)(q^2-q)(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3).$$

On voit aussitôt que $|A|$, $|G: B|$ sont impairs. Il est clair que B normalise A, ce qui signifie que l'indice $|G: N_G(A)|$ est impair. Si φ est une factorisation de G par son centre Z, l'ordre du sous-groupe A^φ et l'indice de son normalisateur dans G^φ sont impairs, eux aussi, i.e. A^φ est un 2-signalisateur dans $\mathbf{PSL}_7(q)$. Or, $A \cap Z = 1$. Par suite, le groupe A^φ est isomorphe à A, donc non abélien.

CHAPITRE 5

GROUPES LIBRES ET VARIÉTÉS

§ 14. Groupes libres

Au commencement du chap. 3 nous avons défini la notion de groupe libre dans une classe donnée et établi que les groupes libres existent et se laissent décrire d'une façon claire dans la classe des groupes abéliens. Dans le présent paragraphe, nous démontrerons l'existence des groupes libres dans la classe de tous les groupes, donnerons leur description et étudierons leurs propriétés élémentaires.

14.1. Définition. Les éléments de l'ensemble générateur M de tout groupe donné G peuvent être liés par des relations dans G, i.e. les produits de chaque élément par son inverse peuvent être égaux à l'unité dans G. Par exemple, $xx^{-1} = e$, $x^{-1}x = e$ pour tout x de M. Découlant des axiomes, les relations indiquées ont toujours lieu dans tous les groupes et s'appellent de ce fait *relations triviales*. Il existe même des groupes qui n'admettent, dans un ensemble générateur, aucune relation non triviale: ils sont « exempts des relations ». Le but de ce n° est de construire de tels groupes et de montrer que ce sont précisément les groupes libres dans la classe de tous les groupes au sens de la définition générale donnée dans le chap. 3 (ce qui explique en particulier l'origine du terme « libre »).

Soit I un ensemble. Quel que soit le groupe G engendré par les x_i, $i \in I$, ses éléments se représentent par des mots $x_{i_1}^{\varepsilon_1} \ldots x_{i_m}^{\varepsilon_m}$, $\varepsilon_j = \pm 1$, et leur multiplication, par la juxtaposition des mots. Cela suggère l'idée de la construction: il faut prendre comme éléments du groupe les mots mêmes formés de lettres $\{x_i, x_i^{-1} \mid i \in I\}$ sans sous-mots du type $x_i^{\varepsilon} x_i^{-\varepsilon}$, $\varepsilon = \pm 1$; multiplier les mots revient alors à les juxtaposer et à éliminer ensuite les sous-mots indiqués.

Plus exactement, prendrons deux ensembles de symboles

$$X = \{x_i \mid i \in I\} \text{ et } X^{-1} = \{x_i^{-1} \mid i \in I\}.$$

Un *mot* écrit *en alphabet* X est une suite vide (notée 1) ou finie de symboles appartenant à $X \cup X^{-1}$. Le nombre d'éléments de la suite s'appelle *longueur* du mot. Nous disons que le mot est *réductible*

s'il contient des symboles voisins du type x_i^{ε}, $x_i^{-\varepsilon}$, $\varepsilon = \pm 1$. Par exemple, le premier des mots

$$x_2x_1x_1x_2^{-1}x_3, \quad x_1x_2x_2^{-1}x_3$$

est irréductible et le second est réductible. Deux mots u, v sont dits *équivalents* (notation $u \sim v$) si v se laisse déduire de u moyennant un nombre fini d'intercalations et de suppressions des mots du type $x_i^{\varepsilon}x_i^{-\varepsilon}$. Il est clair que la relation $\sim$ est réflexive, symétrique et transitive. L'ensemble des mots équivalents à u représente une classe d'équivalence que nous désignons par $[u]$.

14.1.1. Théorème. *Soit $X = \{x_i \mid i \in I\}$. Dans l'ensemble* $\mathbf{F}(X)$ *des classes de mots équivalents écrits en alphabet X, introduisons l'opération de multiplication définie par la loi $[u]\,[v] = [uv]$. Cette définition ne dépend pas du choix arbitraire des représentants dans les classes. L'ensemble* $\mathbf{F}(X)$ *est un groupe pour la multiplication ainsi définie.*

Démonstration. a) Toute classe de mots équivalents contient un seul mot irréductible. En effet, soit $\rho(u)$ un mot irréductible déduit de u en éliminant un à un les sous-mots de droite $x_i^{\varepsilon}x_i^{-\varepsilon}$. La fonction ρ possède les propriétés suivantes (le signe $\equiv$ désigne l'égalité graphique):

$$\rho(u) \sim u, \tag{1}$$

$$\rho(u) \equiv u \quad \text{si } u \text{ est irréductible}, \tag{2}$$

$$\rho(uv) \equiv \rho(u\rho(v)), \tag{3}$$

$$\rho(x_i^{\varepsilon}x_i^{-\varepsilon}u) \equiv \rho(u) \quad \text{pour } \varepsilon = \pm 1, \tag{4}$$

$$\rho(ux_i^{\varepsilon}x_i^{-\varepsilon}v) \equiv \rho(uv) \quad \text{pour } \varepsilon = \pm 1, \tag{5}$$

$$\rho(uv) \equiv \rho(\rho(u)\,\rho(v)). \tag{6}$$

Les propriétés (1), (2), (3) sont des conséquences immédiates de la définition de ρ, (4) découle de (3), la formule (5) résulte de (3), (4), la formule (6) de (3), (4), (5) par récurrence sur la longueur de u. Soit maintenant $u \sim v$, où u, v sont deux mots irréductibles. Il existe par définition une suite de mots

$$u \equiv u_1, \quad u_2, \ldots, u_m \equiv v,$$

où les mots voisins se déduisent l'un de l'autre par intercalation ou suppression d'un sous-mot du type $x_i^{\varepsilon}x_i^{-\varepsilon}$. En vertu de (5) on a $\rho(u_{i+1}) \equiv \rho(u_i)$, donc $\rho(v) \equiv \rho(u)$. Puisque les mots u, v sont irréductibles, il en résulte que $v \equiv u$.

b) Le fait que le produit $[u]\,[v]$ soit indépendant du choix arbitraire des représentants u, v découle de a) et de la formule (6). L'as-

sociativité de la multiplication est immédiate par définition. L'unité sera constituée par la classe qui contient le mot vide, et l'inverse de la classe $[x_{i_1}^{\varepsilon_1}, \ldots, x_{i_m}^{\varepsilon_m}]$, par la classe $[x_{i_m}^{-\varepsilon_m}, \ldots, x_{i_1}^{-\varepsilon_1}]$. Le théorème est démontré.

Le groupe $\mathbf{F}(X)$ s'appelle *groupe libre à ensemble générateur libre* X; le cardinal $|X|$ s'appelle *degré* (*de liberté*) du groupe. Si $X = \{x_1, \ldots, x_n\}$, $X = \{x_1, x_2, \ldots\}$, au lieu de $\mathbf{F}(X)$ on écrit $\mathbf{F}_n(X)$, $\mathbf{F}_\infty(X)$ respectivement. Si les désignations des générateurs n'ont pas d'importance, on écrit $\mathbf{F}_n$, $\mathbf{F}_\infty$ tout court. Dans le texte qui suit, pour désigner les éléments d'un groupe libre, nous utiliserons les représentants des classes, i.e. nous écrirons par exemple $u = v$, $uv = w$ au lieu de $[u] = [v]$, $[u][v] = [w]$. Compte tenu de la remarque a), on peut parler aussi de la notation irréductible d'une classe: on entend par là la notation irréductible $\rho(u)$ de son représentant quelconque u.

14.1.2. Exercice. Les groupes libres de degré $\geqslant 2$ sont non commutatifs.

14.1.3. Exercice. Si u est un mot non vide, la longueur du mot $\rho(u^n)$, $n \geqslant 2$, est plus grande que celle des mots $\rho(u)$, $\rho(u^{-1})$. En particulier, tout groupe libre est un groupe sans torsion.

14.1.4. Exercice. Nous disons d'un mot irréductible qu'il est *cycliquement irréductible* s'il commence par un symbole x_i^{ε} et se termine par un symbole autre que $x_i^{-\varepsilon}$. Eliminant au commencement et à la fin du mot les symboles identiques qui interviennent avec des exposants différents, on réussit à amener tout mot irréductible u, par un nombre fini de pas, à une forme cycliquement irréductible $\sigma(u)$. Montrer que deux éléments u, v d'un groupe libre sont conjugués dans ce groupe si et seulement si $\sigma(u) \equiv w_1 w_2$, $\sigma(v) \equiv w_2 w_1$ pour certains w_1, w_2.

Il se trouve que tout groupe engendré par un ensemble de cardinal n est une image homomorphe d'un groupe libre de degré n. On peut faire mieux: le théorème suivant montre que les groupes $\mathbf{F}(X)$ sont précisément les groupes libres dans la classe de tous les groupes au sens de la définition citée au commencement du chapitre 3.

14.1.5. Théorème. *Soit un groupe G engendré par un ensemble $M = \{g_i \mid i \in I\}$. Choisissons un alphabet $X = \{x_i \mid i \in I\}$. L'application $X \to M$ définie par $x_i \mapsto g_i$ se laisse prolonger d'une façon unique en homomorphisme $\mathbf{F}(X) \to G$.*

Démonstration. Il est clair que la classe $[x_{i_1}^{\varepsilon_1} \ldots x_{i_m}^{\varepsilon_m}]$ doit admettre comme image l'élément $g_{i_1}^{\varepsilon_1} \ldots g_{i_m}^{\varepsilon_m}$. L'univocité et

la nature homomorphe de cette application découlent des définitions. Le théorème est démontré.

Les éléments du noyau H de l'homomorphisme $\mathrm{F}(X) \to G$ s'appellent *relations fondamentales* ou *relateurs* de G sur X. Si un ensemble de relations H' est tel que le plus petit sous-groupe normal de $\mathrm{F}(X)$ contenant H' se confond avec H, on dit que H' est l'*ensemble des relations fondamentales sur* X. Puisque $G \simeq \mathrm{F}(X)/H$, définir l'alphabet X et l'ensemble H' revient à définir complètement le groupe G. Le couple X, H' s'appelle *code génétique* ou *présentation* du groupe G; la notation symbolique est $G = \mathrm{gr}\,(X \parallel H')$. Pour abréger, on omet quelquefois d'énumérer les éléments générateurs, étant sous-entendu que le groupe est engendré par tous les éléments figurant dans les relations fondamentales. Il va sans dire qu'un même groupe admet plus d'un code génétique; l'utilité de tel ou tel code génétique est fonction du problème posé. Un intérêt particulier est représenté par les groupes admettant un code génétique fini, dits *groupes de présentation finie*.

Dans la notation d'un code génétique, au lieu des mots u de H', on écrit parfois les égalités $u = 1$ et même $u_1 = u_2$ si u est de la forme $u_1 u_2^{-1}$.

14.1.6. Exercice. Un groupe abélien libre de degré n admet un code génétique suivant:

$$\mathrm{gr}\,(x_1, \ldots, x_n \parallel x_i^{-1} x_j^{-1} x_i x_j, \quad 1 \leqslant i < j \leqslant n).$$

14.1.7. Exercice:

$$\mathrm{C}_2 \times \mathrm{C}_2 = \mathrm{gr}\,(x, y \parallel x^2 = 1, \quad y^2 = 1, \quad xy = yx).$$

La recherche d'un code génétique du groupe est souvent simplifiée par la *méthode de recensement des classes suivant un sous-groupe*; nous illustrerons cette méthode sur l'exemple du groupe S_4. On commence par choisir des éléments générateurs du groupe considéré et écrire certaines relations entre eux, de façon à avoir la certitude (peut-être intuitive) que les relations choisies définissent bien le groupe. Par exemple, dans le groupe S_4 on peut retenir comme générateurs les éléments $x = (1234)$, $y = (12)$ (voir l'exercice 2.2.4). Puisque $xy = (234)$, on a

$$x^4 = 1, \quad y^2 = 1, \quad (xy)^3 = 1.$$

Le groupe en question n'étant pas compliqué, il y a lieu de supposer que ces trois relations le définissent suffisamment bien. Pour le démontrer, considérons le groupe

$$G = \mathrm{gr}\,(x, y \parallel x^4 = 1, \quad y^2 = 1, \quad (xy)^3 = 1),$$

choisissons dans G un sous-groupe quelconque, par exemple $H = (x)$, et essayons de montrer que G contient $|S_4| : 4 = 6$ classes suivant H. On a alors

$$|G| = |H| \cdot |G : H| = 24;$$

or, puisque S_4 est une image homomorphe de G, on obtient l'isomorphisme cherché $G \simeq S_4$.

Conformément aux relations fondamentales du groupe G, composons trois tableaux

x	x	x	x			y	y			x	y	x	y	x	y		
1	1	1	1	1		1		1		1	1					1	

et commençons le recensement des classes de G suivant H en désignant H lui-même par le chiffre 1. L'égalité évidente $1x = 1$ figure déjà dans tous les tableaux. Quelle relation doit figurer à la place vide dans le deuxième tableau? Posons $1y = 2$, il vient alors $2y = 1$. Mettons ces relations dans tous les tableaux en commençant une nouvelle ligne dans chacun:

x	x	x	x			y		y		x	y	x	y	x	y		
1	1	1	1	1		1	2	1		1	1	2			2	1	
2				2		2	1	2		2			2	1	1	2	

Posons ensuite $2x = 3$, $3x = 4$. Les tableaux deviennent

x	x	x	x			y		y		x	y	x	y	x	y		
1	1	1	1	1		1	2	1		1	1	2	3		2	1	
2	3	4		2		2	1	2		2	3		2	1	1	2	
3	4		2	3		3		3		3	4					3	
4		2	3	4		4		4		4						4	

Soit maintenant $4x = 5$, alors on a $5x = 2$ du premier tableau, $3y = 5$ du troisième et $5y = 3$ du deuxième. Il vient

x	x	x	x	x	y	y		x	y	x	y	x	y
1	1	1	1	1	1	2	1	1	1	2	3	5	2	1
2	3	4	5	2	2	1	2	2	3	5	2	1	1	2
3	4	5	2	3	3	5	3	3	4			4	5	3
4	5	2	3	4	4		4	4	5	3	4			4
5	2	3	4	5	5	3	5	5	2	1	1	2	3	5

Les tableaux deviennent visiblement plus étoffés, ce qui annonce la fin proche du processus de recensement des classes du groupe (dans le cas contraire, les tableaux deviennent clairsemés à mesure que le nombre des lignes croît). Posons maintenant $4y = 6$, cela nous donne

x	x	x	x	x	y	y		x	y	x	y	x	y
1	1	1	1	1	1	2	1	1	1	2	3	5	2	1
2	3	4	5	2	2	1	2	2	3	5	2	1	1	2
3	4	5	2	3	3	5	3	3	4	6	6	4	5	3
4	5	2	3	4	4	6	4	4	5	3	4	6	6	4
5	2	3	4	5	5	3	5	5	2	1	1	2	3	5
6	6	6	6	6	6	4	6	6	6	4	5	3	4	6

Les tableaux sont clos: le recensement des classes du groupe est fini. Son résultat est $|G:H| = 6$. Remarquons que si nous avions manqué, à un pas quelconque, l'occasion de remplir une lacune, une certaine classe se verrait attribuer de différents numéros. Donc, la clôture des tableaux ne nous permet d'écrire rien d'autre que l'inégalité $|G:H| \leqslant 6$. Or, puisque G admet S_4 pour image homomorphe, l'inégalité stricte est en réalité impossible.

Remarquons en outre que la 3e, la 4e et la 5e ligne du premier tableau sont des conséquences de la 2e ligne et peuvent donc être omises; il en est de même pour la 2e, la 5e et la 6e ligne du deuxième tableau et la 2e, la 4e, la 5e et la 6e ligne du troisième tableau. Ces simplifications de la méthode, ainsi que certaines autres, ont cependant un caractère technique et nous ne les décrirons pas ici. Ajoutons seulement que la méthode de recensement décrite est facilement programmable et réalisable sur ordinateur.

14.1.8. Exercice:

$$S_3 = \mathrm{gr}\,(x,\ y \parallel x^2 = y^3 = (xy)^2 = 1).$$

14.1.9. Exercice. Recenser les cinq classes du groupe

$$G = \mathrm{gr}\,(x,\ y,\ z \,\|\, x^3 = y^3 = z^3 = (yz)^2 = (zx)^2 = (xy)^2 = 1)$$

suivant le sous-groupe $H = \mathrm{gr}\,(x,\ y)$.

14.1.10. Exercice. Chercher le code génétique d'un groupe d'ordre pq où p, q sont des nombres premiers tels que $p < q$.

14.1.11. Exercice. Le sous-groupe engendré dans $\mathrm{F}\,(x,\ y)$ par les éléments $x^n y x^n$, $n = 0, 1, 2, \ldots$, est librement engendré par eux (i.e. se définit par un ensemble de relations vide).

La définition des groupes par leurs codes génétiques apparaît naturellement en topologie (par exemple, en théorie des nœuds) et dans d'autres domaines. Une théorie détaillée est donnée dans [8, 23].

14.2. Représentation matricielle. Dans ce n° nous démontrerons qu'il existe un homomorphisme injectif d'un groupe libre dénombrable dans $\mathrm{SL}_2\,(\mathbb{Z})$. Puisque les groupes F_1, F_2, ... se plongent dans F_∞, et F_∞ se plonge dans F_2 (exercice 14.1.11), il suffit de trouver dans $\mathrm{SL}_2\,(\mathbb{Z})$ un sous-groupe libre de degré 2.

14.2.1. Théorème. *Soit m entier, $m \geqslant 2$. Le sous-groupe engendré dans $\mathrm{SL}_2\,(\mathbb{Z})$ par les transvections*

$$t_{12}\,(m) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \quad t_{21}\,(m) = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$$

est librement engendré par elles, i.e. défini par un ensemble de relations vide.

Démonstration. Désignons pour abréger $a = t_{12}\,(m)$, $b = t_{21}\,(m)$. Soit w un produit alterné de puissances non nulles des éléments a, b dans le groupe $\mathrm{SL}_2\,(\mathbb{Z})$. Il s'agit de montrer que $w \neq e$. Si w commence par une puissance de b, on peut conjuguer w par cette puissance et considérer le produit obtenu qui commence, lui, déjà par une puissance de a. Soit donc $w = a^{\alpha_1} b^{\alpha_2} \ldots c^{\alpha_r}$, où $c = a$ ou b, tous les $\alpha_i \neq 0$. Soit z_i la première ligne de la matrice $a^{\alpha_1} b^{\alpha_2} \ldots c^{\alpha_i}$. Si $z_{2k-1} = (x_{2k-1},\ x_{2k})$, on a

$$z_{2k} = z_{2k-1} b^{\alpha_{2k}} = (x_{2k+1},\ x_{2k}), \qquad z_{2k+1} = z_{2k} a^{\alpha_{2k+1}} = (x_{2k+1},\ x_{2k+2}),$$

où

$$x_{2k+1} = x_{2k-1} + m\alpha_{2k} x_{2k}, \quad x_{2k+2} = x_{2k} + m\alpha_{2k+1} x_{2k+1}.$$

La réunion des deux dernières formules nous donne

$$x_{i+2} = x_i + m\alpha_{i+1} x_{i+1} \quad \text{pour} \quad i = 1, 2, \ldots, r-1.$$

Il suffit de montrer que les $|x_i|$ croissent quand i passe de 1 à $r+1$. Pour $i = 1, 2,$ la proposition est immédiate. Ensuite, raisonnons par récurrence:

$$|x_{i+2}| \geqslant m\,|\alpha_{i+1}|\,|x_{i+1}| - |x_i| \geqslant$$
$$\geqslant 2\,|x_{i+1}| - |x_i| \geqslant |x_{i+1}| + 1.$$

Le théorème est démontré.

Les injections canoniques $\mathbf{F}_2 \to \mathbf{SL}_2(\mathbb{Z})$ indiquées dans le théorème s'avèrent fort utiles en théorie des groupes libres. A titre d'illustration, citons une application.

14.2.2. Théorème. *Soit p un nombre premier. Tout groupe libre $\mathbf{F}(X)$ admet une approximation par des p-groupes finis.*

Démonstration. Soit X' une partie finie de X. Appliquant tous les autres générateurs libres dans l'élément unité, nous obtenons l'homomorphisme $\mathbf{F}(X) \to \mathbf{F}(X')$. Puisque l'intersection des noyaux de tels homomorphismes est égale à l'unité, $\mathbf{F}(X)$ est produit sous-cartésien de groupes libres dénombrables d'après le théorème de Remak 4.3.9. On peut donc admettre que $\mathbf{F}(X)$ est dénombrable et se plonge, en vertu du théorème 14.2.1, dans le sous-groupe de congruence $\Gamma_2(p)$. Rappelons (voir l'exercice 4.2.7) qu'on a par définition

$$\Gamma_2(m) = \{x \mid x \in \mathbf{SL}_2(\mathbb{Z}), \quad x \equiv e \pmod{m}\}.$$

Etant noyaux des homomorphismes $\mathbf{SL}_2(\mathbb{Z}) \to \mathbf{SL}_2(\mathbb{Z}_{p^k})$, les sous-groupes $\Gamma_2(p^k)$ sont des sous-groupes normaux d'indices finis dans $\mathbf{SL}_2(\mathbb{Z})$ et leur intersection est évidemment égale à l'unité, $k = 1, 2, \ldots$ Toujours d'après le théorème de Remak, $\Gamma_2(p)$ est donc produit sous-cartésien de groupes finis $\Gamma_2(p)/\Gamma_2(p^k)$. Enfin,

$$(e + pz)^p = \sum_{i=0}^{p} \binom{p}{i} (pz)^i \equiv e \pmod{p^2},$$

$$(e + p^2z)^p = \sum_{i=0}^{p} \binom{p}{i} (p^2z)^i \equiv e \pmod{p^3},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

donc $\Gamma_2(p)/\Gamma_2(p^k)$ est un p-groupe. Le théorème est démontré.

Nous attirons l'attention du lecteur sur le fait que l'approximabilité finie des groupes libres vient d'être déduite de celle du groupe $\mathbf{GL}_n(\mathbb{Z})$. Plus généralement, on réussit souvent à déduire l'approximabilité finie d'un groupe à partir de sa représentabilité par des matrices en s'appuyant sur le théorème suivant dû à A. I. Mal-

tsev (*Matem. sb.*, 1940, 8, n° 3, p. 405-421) : *tout groupe de matrices de type fini sur un corps commutatif admet une approximation finie.* Le lecteur trouvera une démonstration bien simple de ce théorème dans [25], p. 408.

On vérifie aisément que l'ensemble

$$G_m = \{x \mid x \in \mathrm{SL}_2(\mathbb{Z}),\quad x_{11} \equiv x_{22} \equiv 1 \pmod{m^2},\quad x_{12} \equiv x_{21} \equiv 0 \pmod{m}\}$$

est un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ et que

$$\mathrm{gr}\,(t_{12}(m),\quad t_{21}(m)) \leqslant G_m.$$

Dans le cas général, on a l'inégalité stricte, mais, comme l'a montré I. N. Sanov (*Doklady Akad. naouk SSSR*, 1947, 57, n° 7, p. 657-659),

$$\mathrm{gr}\,(t_{12}(2),\quad t_{21}(2)) = G_2,$$

i.e. toute matrice de G_2 se laisse décomposer en produit de puissances des transvections $a = t_{12}(2)$ et $b = t_{21}(2)$. L'idée d'une telle décomposition est suggérée par les formules

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} a^{\alpha} = \begin{pmatrix} x_{11} & x_{12} + 2\alpha x_{11} \\ x_{21} & x_{22} + 2\alpha x_{21} \end{pmatrix},$$

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} b^{\beta} = \begin{pmatrix} x_{11} + 2\beta x_{12} & x_{12} \\ x_{21} + 2\beta x_{22} & x_{22} \end{pmatrix}.$$

Nous nous bornerons à l'illustrer sur l'exemple de la matrice

$$x = \begin{pmatrix} -23 & -86 \\ -4 & -15 \end{pmatrix}.$$

Ici $|x_{12}| > |x_{11}|$. Cherchons un α tel que dans la matrice $x' = xa^{\alpha}$ il y ait $|x'_{12}| < |x'_{11}|$. A cet effet, divisons $x_{12} + |x_{11}|$ par $2x_{11}$ avec reste : $-63 = (-46)\,2 + 29$. Prenons $\alpha = -2$ (le quotient avec le signe inverse). Il vient

$$x' = xa^{-2} = \begin{pmatrix} -23 & 6 \\ -4 & 1 \end{pmatrix}.$$

Cherchons à présent un β tel que dans la matrice $x'' = x'b^{\beta}$ il y ait $|x''_{12}| > |x''_{11}|$. Divisons $x''_{11} + |x'_{12}|$ par $2x'_{12}$ avec reste : $-17 = 12\,(-2) + 7$. Prenons $\beta = 2$ (le quotient avec le signe inverse). Il vient

$$x'' = x'b^2 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} = a^3.$$

On a donc $x = a^3 b^{-2} a^2$.

14.2.3. Exercice. Décrire et justifier l'algorithme de décomposition des matrices de G_2 suivant les générateurs $t_{12}(2)$, $t_{21}(2)$. A l'aide de cet algorithme, décomposer la matrice $\begin{pmatrix} 321 & -86 \\ 698 & -187 \end{pmatrix}$.

14.3. Sous-groupes. Il se trouve que tout sous-groupe d'un groupe libre est lui-même libre. Ce théorème fut démontré en 1921 par J. Nielsen pour les groupes de type fini, et en 1927 par O. Schreier pour le cas général. Dans ce n° nous décrivons la méthode de Schreier qui permet de trouver un système de générateurs libres pour tout sous-groupe d'un groupe libre.

Soit H un sous-groupe d'un groupe quelconque G. Choisissons un représentant de chaque classe à droite de G suivant H. Le représentant pour H sera 1. Une fonction qui prend sur toute classe à droite une valeur constante — un représentant fixe de la classe — s'appelle *fonction de choix* ou *fonction représentative* (à droite). On vérifie immédiatement les propriétés suivantes de cette fonction: $\bar{\bar{u}} = \bar{u}$ et $\overline{\bar{u}v} = \overline{uv}$, où $u, v \in G$ et $\bar{u}$ est un représentant fixe de la classe Hu.

La fonction de choix permet de construire les éléments générateurs du sous-groupe à partir de ceux du groupe.

14.3.1. Théorème. *Soient M l'ensemble générateur d'un groupe G, H un sous-groupe de G, $u \to \bar{u}$ la fonction de choix à droite dans G suivant H, S l'ensemble des représentants choisis. Alors*

$$H = \mathrm{gr}\,(sx\overline{sx}^{-1} \mid s \in S, \quad x \in M).$$

Démonstration. Il est clair que les éléments $sx\overline{sx}^{-1}$ sont contenus dans le sous-groupe H. Montrons que tout élément de H se laisse mettre sous la forme d'un produit des éléments $sx\overline{sx}^{-1}$ et de leurs inverses. On vérifie immédiatement que

$$(sx\overline{sx}^{-1})^{-1} = s'x^{-1}\overline{s'x^{-1}}^{-1}, \quad \text{où } s' = \overline{sx};$$

remarquons que de s' on déduit d'une façon unique $s = \overline{s'x^{-1}}$. Soit maintenant un élément $u = x_1^{\varepsilon_1} \ldots x_r^{\varepsilon_r}$, $x_i \in M$, $\varepsilon_i = \pm 1$, tiré de H. Il s'agit de le mettre sous la forme d'un mot construit avec des éléments de la forme $sx\overline{sx}^{-1}$. Désignons $u_1 = 1$, $u_{i+1} = x_1^{\varepsilon_1} \ldots$ $\ldots x_i^{\varepsilon_i}$. La notation cherchée sera alors

$$u = (\bar{u}_1 x_1^{\varepsilon_1} \overline{u_1 x_1^{\varepsilon_1}}^{-1})\,(\bar{u}_2 x_2^{\varepsilon_2} \overline{u_2 x_2^{\varepsilon_2}}^{-1}) \ldots (\bar{u}_r x_r^{\varepsilon_r} \overline{u_r x_r^{\varepsilon_r}}^{-1}). \tag{1}$$

En effet,

$$\overline{u_i x_i^{\varepsilon_i}}^{-1}\, \overline{u_{i+1}} = 1, \quad i = 1, \ldots, r-1,$$

aussi le second membre de (1) s'écrit-il

$$\bar{u}_1 u \overline{u_r x_r^{\varepsilon_r}}^{-1} = 1 \cdot u \cdot \bar{u}^{-1} = 1 \cdot u \cdot 1 = u.$$

Le théorème est démontré.

14.3.2. Exercice. Tout sous-groupe d'indice fini dans un groupe de type fini est de type fini.

14.3.3. Exercice. Chercher dans le groupe libre $\mathbf{F}_n$ les éléments générateurs du sous-groupe des mots de longueur paire.

14.3.4. Exercice. Utilisant la démonstration du théorème 14.3.1 et la formule de l'exercice 2.2.4, chercher un ensemble générateur de $\mathbf{A}_n$.

Un ensemble d'éléments représentés par des mots irréductibles dans un groupe libre est appelé *système schreiérien* s'il contient, avec chaque son élément, tous ses segments initiaux.

14.3.5. Théorème (Nielsen-Schreier). *Soient X un alphabet quelconque et H un sous-groupe quelconque dans le groupe libre $F = \mathbf{F}(X)$. Il existe au moins un système schreiérien de représentants de F suivant H. Si $u \mapsto \bar{u}$ est la fonction de choix correspondante, H est librement engendré par les éléments non triviaux $s\overline{sx}^{-1}$, où s parcourt l'ensemble des représentants choisis et x parcourt X.*

Démonstration. a) Existence d'un système schreiérien de représentants à droite. On appelle *longueur d'une classe* de F *suivant* H la longueur de son mot le plus court. Construisons le système schreiérien par récurrence sur la longueur de la classe.

Choisissons comme représentant pour H le mot vide. Si L est une classe de longueur 1, choisissons un mot quelconque de longueur 1 comme représentant de L. Supposons que les représentants des classes de longueur inférieure à r soient déjà choisis, i.e. qu'une fonction de choix $u \mapsto \bar{u}$ soit déjà définie sur ces classes, la longueur du représentant étant égale à celle de la classe. Soit L une classe quelconque de longueur r. Choisissons dans L un mot quelconque $y_1 \ldots y_r$, $y_i \in X \cup X^{-1}$, et prenons comme représentant de L le mot $\overline{y_1 \ldots y_{r-1}} y_r$. Il est clair qu'un système de représentants ainsi construit est un système schreiérien.

b) Soit S un système schreiérien de représentants de F suivant H, et soit $u \mapsto \bar{u}$ la fonction de choix qui correspond à S. Montrons que les éléments $\neq 1$

$$s\overline{sx}^{-1}, \quad s \in S, \quad x \in X, \tag{2}$$

engendrent librement H. On sait déjà qu'ils engendrent H, conformément au théorème 14.3.1. Il reste à montrer que ces éléments ne sont pas liés par des relations non triviales.

Tout d'abord, chaque mot (2) est irréductible. En effet, les réductions ne peuvent commencer qu'aux jonctions avec la lettre x. Or, si $s \equiv s_1x^{-1}$, on aurait $sx\overline{sx}^{-1} = s_1\overline{s_1}^{-1} = 1$, et si $\overline{sx}^{-1} \equiv x^{-1}s_2^{-1}$, on aurait $s = s_2$ et $sx\overline{sx}^{-1} = 1$.

Soient ensuite u, v deux mots $\neq 1$ de la forme (2) ou leurs inverses, tels que $uv \neq 1$. De la démonstration du théorème 14.3.1 il ressort que

$$u = sx^{\varepsilon}\overline{sx^{\varepsilon}}^{-1}, \quad v = ty^{\delta}\overline{ty^{\delta}}^{-1}, \quad s,\ t \in S, \quad x,\ y \in X, \quad \varepsilon,\ \delta = \pm 1.$$

Puisque les mots u, v sont irréductibles, le processus des réductions dans le produit uv ne peut commencer qu'à la jonction. Il s'arrêtera avant d'atteindre x^{ε} à gauche et y^{δ} à droite. En effet, puisque les représentants choisis forment un système schreiérien, si le processus des réductions commençait par x^{ε}, l'on aurait $t \equiv s_1x^{-\varepsilon}w$, où $s_1 \equiv \overline{sx^{\varepsilon}}$, d'où

$$s_1x^{-\varepsilon} \equiv \overline{s_1x^{-\varepsilon}} = s.$$

Or, cela est impossible, car $u \neq 1$. Si le processus des réductions commençait par y^{δ}, l'on aurait $s_1 \equiv ty^{\delta}w$, où $s_1 \equiv \overline{sx^{\varepsilon}}$, d'où

$$ty^{\delta} = \overline{ty^{\delta}}.$$

Or, cela est impossible, car $v \neq 1$. Enfin, la réduction simultanée de x^{ε}, y^{δ} est aussi impossible, car $uv \neq 1$.

Soit maintenant un mot irréductible non vide écrit avec des symboles du type (2). Il s'agit de montrer que, considéré comme un mot sur X et soumis à toutes les réductions possibles, il reste un mot non vide. En effet, en vertu de ce que nous venons de voir, les réductions ne peuvent commencer qu'aux jonctions des mots (2) et s'arrêtent avant d'atteindre leurs cœurs x. Le théorème est démontré.

14.3.6. Exercice. Chercher dans $\mathbf{F}(x, y)$ un système de représentants schreiériens, à l'aide de celui-ci, trouver des générateurs libres pour le commutant et pour le plus petit sous-groupe normal contenant x, y^r, où r est un entier.

Le théorème suivant permet de calculer les degrés de liberté des sous-groupes d'indice fini dans les groupes libres de degré fini.

14.3.7. Théorème. *Soient* $F = \mathbf{F}(x_1, \ldots, x_n)$, $H \leqslant F$, $|F : H| = j$. *Si* n, j *sont des nombres finis, le degré de* H *est*

$$m = 1 + (n - 1)j.$$

Démonstration. Soit, dans les notations du théorème précédent, M l'ensemble de toutes les nj notations de la forme (2). Il s'agit d'indiquer les cas où ces notations sont équivalentes

à l'unité. A cet effet, désignons par S_0 l'ensemble S sans l'unité et définissons une application $\tau: S_0 \to M$ telle que

$$s^\tau = \begin{cases} s'\overline{xs'x}^{-1} & \text{pour } s \equiv s'x, \quad x \in X, \\ s\overline{xsx}^{-1} & \text{pour } s \equiv s'x^{-1}, \quad x \in X. \end{cases}$$

On vérifie immédiatement que τ est une application bijective de S_0 sur les notations équivalentes à l'unité dans M. Puisque le degré de H est égal au nombre des notations qui restent, i.e. $nj - (j - 1)$, le théorème est démontré.

14.3.8. Exercice. Un sous-groupe d'indice fini dans un groupe libre de degré infini a lui-même un degré de liberté infini.

14.3.9. Exercice. Si F_1, F_2 sont deux sous-groupes libres de même indice fini dans un groupe G, on a $F_1 \simeq F_2$.

14.4. Séries centrales et séries dérivées. Soit G un groupe quelconque. Définissons dans G une suite décroissante de sous-groupes

$$\gamma_1 G \geqslant \gamma_2 G \geqslant \ldots \tag{3}$$

telle que $\gamma_1 G = G$ et que, pour un sous-groupe $\gamma_n G$ déjà défini, il y ait $\gamma_{n+1} G = [\gamma_n G, G]$; ici $[A, B]$ est le commutant réciproque des groupes A et B. La suite de sous-groupes obtenue s'appelle *série centrale inférieure*, et son terme $\gamma_n G$, *n-ième terme central inférieur* du groupe G. L'intersection de tous les sous-groupes de la série (3) est le *ω-ième terme central inférieur* de G.

Les mots

$$\gamma_1 (x_1) = x_1,$$

$$\gamma_{n+1} (x_1, \ldots, x_{n+1}) = [\gamma_n (x_1, \ldots, x_n), x_{n+1}], \qquad n = 1, 2, \ldots,$$

s'appellent *commutateurs simples*, et le nombre n, *poids* du commutateur γ_n.

14.4.1. Exercice. Pour tout groupe G

$$\gamma_n G = \mathrm{gr}\,(\gamma_n (g_1, \ldots, g_n) \mid g_i \in G), \quad n = 1, 2, \ldots$$

14.4.2. Exercice. Pour tout groupe G on a

$$[\gamma_i G, \gamma_j G] \leqslant \gamma_{i+j} G, \quad i, j = 1, 2, \ldots$$

Indication. Appliquer le raisonnement par récurrence et le lemme des trois commutants 3.2.3.

14.4.3. Exercice. Pour tout groupe, le n-ième commutant est inclus dans le 2^n-ième terme central inférieur; le n-ième terme central inférieur du sous-groupe est contenu dans le n-ième terme central inférieur du groupe.

14.4.4. Théorème (Magnus). *Dans tout groupe libre F, le ω-ième terme central inférieur est égal à l'unité.*

Démonstration. a) Soit d'abord F dénombrable. En vertu du théorème 14.2.1, le groupe F se plonge dans le sous-groupe de congruence $\Gamma_2(m)$, $m \geqslant 2$; il suffit donc de s'assurer que le ω-ième terme central inférieur de $\Gamma_2(m)$ est égal à l'unité.

Prenons des matrices

$$g = e + m^k a \in \Gamma_2(m^k) \quad \text{et} \quad f = e + m^l b \in \Gamma_2(m^l).$$

Soient $g^{-1} = e + m^k a'$ et $f^{-1} = e + m^l b'$. Alors le commutateur

$$\begin{aligned}[g, f] &= (e + m^k a')(e + m^l b')(e + m^k a)(e + m^l b) = \\ &= e + (m^k a' + m^k a + m^{2k} a' a) + \\ &\quad + (m^l b' + m^l b + m^{2l} b' b) + \ldots = e + \ldots,\end{aligned}$$

où les points de suspension désignent des produits mixtes du type $m^{2k+l} a' a b$. Il est clair que tout produit mixte de ce type est congru à la matrice nulle modulo m^{k+l}, d'où $[g, f] \in \Gamma_2(m^{k+l})$.

Le calcul montre que

$$[\Gamma_2(m^k), \Gamma_2(m^l)] \leqslant \Gamma_2(m^{k+l}),$$

d'où $\gamma_i \Gamma_2(m) \leqslant \Gamma_2(m^i)$. Puisque $\bigcap_i \Gamma_2(m^i) = e$, le théorème est démontré pour les groupes dénombrables.

b) Soit maintenant F un groupe libre quelconque. Supposons que le ω-ième terme central inférieur de F contient un élément $f \neq 1$. Décomposons f pour chaque $n = 1, 2, \ldots$ en produit de commutateurs simples de poids n, réunissons tous les éléments commutables et exprimons-les par l'intermédiaire des éléments générateurs de F. Il est clair que les éléments générateurs utilisés forment alors un ensemble dénombrable. Cet ensemble engendre un sous-groupe libre. Puisqu'il est dénombrable et ne vérifie pas le théorème de Magnus, nous obtenons une contradiction. Le théorème est démontré.

En vertu des résultats de l'exercice 14.4.3, il ressort de ce théorème que le ω-ième commutant d'un groupe libre, i.e. l'intersection de tous les commutants de numéro naturel, est égal à l'unité.

Soit u un mot sur l'alphabet X. On appelle *logarithme de u dans la base $x \in X$* le nombre entier $\log_x u$ égal à la somme des exposants de la lettre x dans le mot u (il est évident que deux mots équivalents ont même logarithme). Il est clair que l'application qui associe à chaque u de $\mathbf{F}(X)$ l'ensemble de ses logarithmes $\log_x u$ pour tous les $x \in X$ est un homomorphisme du groupe libre $\mathbf{F}(X)$ sur un groupe abélien libre de même rang. Puisque les mots de même logarithme pour toutes les bases appartiennent à une même classe suivant le commutant, le commutant $[\mathbf{F}(X), \mathbf{F}(X)]$ sera le noyau de cet homo-

morphisme. Appliquant ce raisonnement au commutant du groupe libre, etc., nous obtenons le résultat suivant:

Les sections de la série dérivée d'un groupe libre sont des groupes abéliens libres.

Remarquons sans démonstration que les sections de la série centrale inférieure d'un groupe libre sont aussi des groupes abéliens libres (théorème de Witt). Ce résultat s'obtient avec des moyens beaucoup plus fins.

14.4.5. Exercice. Deux groupes libres de degrés de liberté différents ne sont pas isomorphes.

14.4.6. Exercice. Utilisant les relations entre commutateurs indiquées dans le n° 3.2, montrer que les sections de la série centrale inférieure d'un groupe libre de degré fini sont des groupes abéliens de type fini.

§ 15. Variétés

On appelle *variétés* les sous-classes définies dans la classe de tous les groupes par des relations identiques. Par exemple, la classe des groupes abéliens est une variété définie par l'identité $xy = yx$. Les variétés sont étroitement liées aux groupes libres, vu que les identités sont éléments de groupes libres. Un grand nombre de travaux sont consacrés à la théorie des variétés, dont l'ouvrage de H. Neumann [26].

Nous introduisons ici quelques notions de base de cette théorie et montrons que les variétés se confondent avec les classes de groupes fermées par rapport à la prise de sous-groupes, d'images homomorphes et de produits cartésiens.

15.1. Identités et variétés. On dit qu'un mot v écrit en alphabet $x_1, x_2, \ldots$ est une *identité* sur la classe de groupes $\mathfrak{L}$ s'il devient unité sur tout groupe G de $\mathfrak{L}$ quand les arguments $x_1, x_2, \ldots$ parcourent G. Soient V un ensemble de mots en alphabet $x_1, x_2, \ldots$, et G un groupe. Dans le cas général, les mots de V ne sont pas forcément des identités sur G, et leurs valeurs sur G engendrent un sous-groupe

$$V(G) = \mathrm{gr}\,(v\,(g_1, \ldots, g_{n(v)}) \mid v \in V,\ g \in G). \tag{1}$$

Ce sous-groupe, dit *sous-groupe verbal* dans G par rapport à V, mesure dans un certain sens l'écart de G par rapport aux groupes de la variété définie par les identités de V. Deux exemples évidents de sous-groupes verbaux sont fournis par le commutant et la puissance d-ième d'un groupe: ils se définissent par les mots $[x, y]$, x^d et mesurent l'écart du groupe par rapport aux groupes commutatifs et aux groupes de période d.

15.1.1. Exercice. Les termes centraux et les commutants successifs d'un groupe sont ses sous-groupes verbaux.

15.1.2. Exercice. Un sous-groupe verbal d'un sous-groupe verbal est encore verbal dans le groupe tout entier.

15.1.3. Exercice. Les sous-groupes verbaux du groupe $\mathbf{F}_\infty$ sont exactement ses parties H qui vérifient les conditions :

1° $u, v \in H \Rightarrow uv \in H$,

2° $u \in H \Rightarrow u^{-1} \in H$,

3° $u \in H, v_1, \ldots, v_{n(u)} \in \mathbf{F}_\infty \Rightarrow u(v_1, \ldots, v_{n(u)}) \in H$.

Démontrons l'existence tout en donnant la description des groupes libres dans une variété quelconque au sens des définitions données au commencement du chapitre 3.

15.1.4. Théorème. *Soit $\mathfrak{L}$ une variété de groupes définie par des identités de V. Soient X un alphabet,*

$$\mathbf{F}_V(X) = \mathbf{F}(X)/V(\mathbf{F}(X)) \tag{2}$$

et $*$ l'homomorphisme canonique $\mathbf{F}(X) \to \mathbf{F}_V(X)$. Si $X = \{x_i \mid i \in I\}$ et G est un groupe dans $\mathfrak{L}$ dont l'ensemble générateur est $\{g_i \mid i \in I\}$, l'application $x_i^* \mapsto g_i$ se laisse prolonger d'une façon unique en homomorphisme $\mathbf{F}_V(X) \to G$. Autrement dit, les groupes $\mathbf{F}_V(X)$ sont libres dans la variété $\mathfrak{L}$. Ils sont les seuls groupes libres dans $\mathfrak{L}$.

Démonstration. a) Il est clair que l'homomorphisme $\mathbf{F}_V(X) \to G$ s'obtient en faisant correspondre à un mot en x_i^* le même mot en g_i. On vérifie immédiatement que cette application est définie d'une façon unique et est un homomorphisme. Par conséquent, $\mathbf{F}_V(X)$ est un groupe libre dans $\mathfrak{L}$.

b) Soit F un groupe dans $\mathfrak{L}$ librement engendré par f_i, $i \in I$. L'application $f_i \to x_i^*$ se laisse prolonger en homomorphisme $F \to \mathbf{F}_V(X)$, et l'application $x_i^* \to f_i$, en homomorphisme $\mathbf{F}_V(X) \to F$, d'où $F \simeq \mathbf{F}_V(X)$. Le théorème est démontré.

L'ensemble $\{x_i^* \mid i \in I\}$ s'appelle *ensemble générateur libre* du groupe $\mathbf{F}_V(X)$, et son cardinal, *degré de liberté* de $\mathbf{F}_V(X)$. Ces notions généralisent les notions analogues que nous avons introduites antérieurement pour les groupes libres et les groupes abéliens libres. Pour un groupe libre de degré n dans une variété $\mathfrak{L}$, on emploie aussi le symbole $\mathbf{F}_n(\mathfrak{L})$.

Une description exhaustive des groupes libres dans la variété des groupes abéliens a été donnée dans le § 7. Dans d'autres variétés, les groupes libres peuvent présenter une structure assez complexe (voir en particulier le § 23).

15.1.5. Exercice. Le groupe des quaternions $\mathrm{gr}(x, y \mid\mid x^4, x^2y^2, x^{-1}yxy)$ n'est libre en aucune variété.

Soit v un mot. On a évidemment

$$v(g_1, \ldots, g_r)^\varphi = v(g_1^\varphi, \ldots, g_n^\varphi)$$

pour tout homomorphisme $\varphi: G \to G^*$, aussi l'image homomorphe du sous-groupe verbal $V(G)$ est-elle contenue dans le sous-groupe verbal $V(G^*)$. En particulier, tout sous-groupe verbal est End-permis.

15.1.6. Exercice. Indiquer dans $C_2 \times C_4$ un sous-groupe End-permis qui ne soit pas verbal.

Pour les groupes libres dans une variété, les choses se présentent plus simplement:

15.1.7. Théorème. *Soit $\mathfrak{L}$ une variété de groupes; G est un groupe libre dans $\mathfrak{L}$. Tout sous-groupe End-permis H de G est verbal.*

Démonstration. Prenons dans G un ensemble générateur libre $\{g_i \mid i \in I\}$ et considérons dans F_∞ un ensemble V de mots $v(x_{i_1}, \ldots, x_{i_m})$ tels que $v(g_{i_1}, \ldots, g_{i_m}) \in H$. Montrons que $H = V(G)$. L'inclusion $H \leqslant V(G)$ est évidente.

Soient réciproquement $v \in V$, $g'_i \in G$. Il s'agit de montrer que

$$v(g'_{i_1}, \ldots, g'_{i_m}) \in H.$$

Or, puisque G est libre dans $\mathfrak{L}$, l'application $g_i \mapsto g'_i$ se laisse prolonger en un endomorphisme de G. Comme $v(g_{i_1}, \ldots, g_{i_m}) \in H$ et H est End-permis, on a $v(g'_{i_1}, \ldots, g'_{i_m}) \in H$. Le théorème est démontré.

La correspondance entre les variétés et les ensembles de mots de F_∞ qui les définissent n'est pas biunivoque, car deux ensembles de mots différents peuvent définir une même variété. D'autre part, l'ensemble de toutes les identités vraies sur la variété donnée a une structure de sous-groupe verbal de F_∞; on voit sans peine que cette correspondance entre variétés et sous-groupes verbaux est biunivoque. Etudier les variétés équivaut donc à étudier les sous-groupes verbaux de F_∞.

15.1.8. Exercice. Le sous-groupe engendré dans F_∞ par des sous-groupes verbaux est verbal. Quelle est la variété qu'il définit?

Deux ensembles d'identités V, W sont dits *équivalents* s'ils définissent une même variété de groupes ou, ce qui revient au même, si $V(F_\infty) = W(F_\infty)$.

15.1.9. Exercice. Tout ensemble d'identités fini est équivalent à une seule identité.

(Remarquons cependant que toute variété de groupes ne peut pas, loin s'en faut, être définie par la donnée d'une seule identité.)

15.1.10. Théorème. *Tout ensemble V de mots en alphabet $x_1, x_2, \ldots$ est équivalent à un ensemble de la forme $W = \{x_1^d, u_j \mid j \in J\}$, où $d \geqslant 0$ et les u_j sont des mots du commutant du groupe* $\mathbf{F}(x_1, x_2, \ldots)$.

Démonstration. Mettons chaque v de V sous la forme

$$v = x_{i_1}^{m_1} \ldots x_{i_s}^{m_s} u,$$

où les symboles $i_1, \ldots, i_s$ sont tous distincts et u est un élément du commutant de $\mathbf{F}(x_1, x_2, \ldots)$. Soit d le pgcd des nombres $m_1, \ldots, m_s$ pour tous les v de V. Le nombre d et les éléments u pris pour tous les v de V sont justement les quantités qu'on cherche. En effet, il est clair que $V(\mathbf{F}_\infty) \leqslant W(\mathbf{F}_\infty)$. Réciproquement, les mots x_{ik}^{mk} sont contenus dans $V(\mathbf{F}_\infty)$ (ils se déduisent de v quand les autres lettres de l'alphabet ont pour image l'unité), ce qui fait que les mots x_1^d, u y sont contenus aussi. Le théorème est démontré.

15.2. Une autre approche des variétés. Soit $\mathfrak{L}$ une classe de groupes; désignons par $S\mathfrak{L}$, $Q\mathfrak{L}$, $C\mathfrak{L}$ les fermetures de $\mathfrak{L}$ par rapport aux opérations de prise de sous-groupes, d'images homomorphes et de produits cartésiens respectivement. Soit maintenant $\mathfrak{L}$ une variété: on a alors de toute évidence $S\mathfrak{L} = \mathfrak{L}$, $Q\mathfrak{L} = \mathfrak{L}$, $C\mathfrak{L} = \mathfrak{L}$. Il se trouve que la réciproque est aussi vraie:

15.2.1. Théorème (Birkhoff). *Soit $\mathfrak{L}$ une classe de groupes. Si $S\mathfrak{L} = \mathfrak{L}$, $Q\mathfrak{L} = \mathfrak{L}$ et $C\mathfrak{L} = \mathfrak{L}$, alors $\mathfrak{L}$ est une variété.*

Démonstration. Soient V l'ensemble de toutes les identités vraies sur $\mathfrak{L}$ et $\overline{\mathfrak{L}}$ la variété qu'elles déterminent. Il est évident que $\mathfrak{L} \subseteq \overline{\mathfrak{L}}$; il s'agit de montrer que $\overline{\mathfrak{L}} \subseteq \mathfrak{L}$. Puisque $Q\mathfrak{L} = \mathfrak{L}$, il suffit de vérifier que tout groupe F libre dans $\overline{\mathfrak{L}}$ appartient à $\mathfrak{L}$; or, puisqu'on a $C\mathfrak{L} = \mathfrak{L}$ et $S\mathfrak{L} = \mathfrak{L}$, il suffit que F se plonge dans un produit cartésien de groupes de $\mathfrak{L}$. Nous allons indiquer un tel plongement.

Conformément au théorème 15.1.4,

$$F = \mathbf{F}(X)/V(\mathbf{F}(X))$$

pour un alphabet convenable $X = \{x_i \mid i \in I\}$. Pour chaque mot $v(x_{i_1}, \ldots, x_{i_m})$ n'appartenant pas à V, prenons dans $\mathfrak{L}$ un groupe G_v et choisissons dans ce G_v des éléments g_{vi}, $i \in I$, tels que

$$v(g_{vi_1}, \ldots, g_{vi_m}) \neq 1.$$

Prenons le produit cartésien

$$\prod_{v \notin V} G_v$$

et considérons dans ce produit le sous-groupe engendré par les éléments f_i, $i \in I$, où $f_i(v) = g_{vi}$. Puisque les éléments f_i ne vérifient aucune relation sauf les identités de V, le sous-groupe qu'ils engendrent est isomorphe à F. Le théorème est démontré.

Il est facile de voir qu'en réalité nous venons de démontrer l'égalité

$$\overline{\mathfrak{L}} = \mathrm{QSC}\mathfrak{L} \tag{3}$$

pour une classe de groupes arbitraire $\mathfrak{L}$.

15.2.2. Exercice. Soient G un groupe fini et $\mathfrak{M}$ la variété définie par toutes les identités vraies sur G. Tout groupe de type fini dans $\mathfrak{M}$ est fini.

Indication: utiliser la formule (3) pour $\mathfrak{L} = \{G\}$.

15.2.3. Exercice. Dans un groupe de type fini G, tout sous-groupe H d'indice fini contient un sous-groupe verbal d'indice fini.

Solution. Conformément à l'exercice 2.5.13, on peut admettre que H est normal dans G. Soient V le système de toutes les identités vraies sur le groupe fini G/H et $\mathfrak{M}$ la variété définie par ces identités. Puisque le groupe $G/V(G)$ est de type fini et appartient à $\mathfrak{M}$, il est fini (exercice 15.2.2).

15.2.4. Exercice. Indiquer les classes de groupes $\mathfrak{L}$, $\mathfrak{M}$, $\mathfrak{N}$ qui vérifient les conditions

$$\begin{array}{lll} \mathrm{S}\mathfrak{L} \neq \mathfrak{L}, & \mathrm{Q}\mathfrak{L} = \mathfrak{L}, & \mathrm{C}\mathfrak{L} = \mathfrak{L}, \\ \mathrm{S}\mathfrak{M} = \mathfrak{M}, & \mathrm{Q}\mathfrak{M} \neq \mathfrak{M}, & \mathrm{C}\mathfrak{M} = \mathfrak{M}, \\ \mathrm{S}\mathfrak{N} = \mathfrak{N}, & \mathrm{Q}\mathfrak{N} = \mathfrak{N}, & \mathrm{C}\mathfrak{N} \neq \mathfrak{N}. \end{array}$$

CHAPITRE 6

GROUPES NILPOTENTS

Dans les chapitres précédents, nous nous sommes familiarisés avec les groupes abéliens et les groupes finis. Un groupe arbitraire, s'il n'appartient pas toujours à ces deux familles, s'y trouve sûrement lié d'une façon ou d'une autre. La recherche du plus grand nombre possible de telles liaisons et l'étude du groupe lui-même par ses liaisons, telle est la méthode habituelle de très nombreux travaux en théorie des groupes. Les auteurs de ces travaux ont inventé tout un éventail de conditions analogues à la commutativité ou à la finitude du groupe, des plus naturelles aux plus fantaisistes, voire aberrantes.

Les généralisations les plus importantes de la commutativité sont la résolubilité et la nilpotence. Les groupes résolubles sont ceux qui se laissent assembler à partir de groupes abéliens par plusieurs extensions successives. Ils sont remarquables en particulier par leur relation avec le problème de résolubilité des équations algébriques par radicaux (voir Introduction), d'où leur appellation.

Les groupes nilpotents constituent une classe à mi-chemin entre les groupes abéliens et les groupes résolubles. Ils sont moins faciles à définir et admettent une étude plus approfondie.

Le présent chapitre sera consacré à l'étude des groupes nilpotents, et le chapitre suivant, à celle des groupes résolubles. Le lecteur trouvera beaucoup de résultats intéressants sur les groupes nilpotents et résolubles dans [21, 14, 16, 37].

§ 16. Propriétés générales et exemples

16.1. Définition. Soit G un groupe. Sa matriochka normale

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_s = G \tag{1}$$

est dite *centrale* si toutes ses sections sont centrales, i.e.

$$G_{i+1}/G_i \leqslant Z\,(G/G_i) \text{ pour tout } i \tag{2}$$

ou, ce qui revient au même,

$$[G_{i+1}, G] \leqslant G_i \text{ pour tout } i. \tag{3}$$

Un groupe qui admet des matriochkas centrales s'appelle *nilpotent* (cette appellation sera expliquée plus tard), et le nombre minimal des sections de telles matriochkas, son *degré de nilpotence*. De la définition, on voit sans peine que les groupes nilpotents forment une classe intermédiaire entre les classes des groupes abéliens et des groupes résolubles et que tout groupe abélien est exactement un groupe nilpotent de degré 1.

16.1.1. Exercice. Toute matriochka de sous-groupes vérifiant la condition (3) est normale.

Soit G un groupe quelconque. Nous tâcherons d'y construire une matriochka centrale en appliquant soit la formule (2), soit la formule (3). Soient en effet

$$\zeta_0 G = 1, \quad \zeta_{i+1}G/\zeta_i G = Z(G/\zeta_i G), \ i = 0, 1, 2, \ldots,$$
$$\gamma_1 G = G, \quad \gamma_{i+1}G = [\gamma_j G, G], \ j = 1, 2, \ldots$$

Les sous-groupes $\zeta_i G$ s'appellent *hypercentres* de G, tandis que les sous-groupes $\gamma_j G$ sont les *termes centraux* de G déjà connus (les uns et les autres se définissent aisément pour des i et j transfinis quelconques, mais nous ne le ferons pas, de peur de nous y embourber). Il est clair que si un hypercentre se confond avec le groupe tout entier ou un terme central se confond avec l'unité, le groupe est nilpotent.

Réciproquement, supposons que le groupe G soit nilpotent et que (1) soit une matriochka centrale quelconque dans G. Désignons abréviativement $Z_i = \zeta_i G$, $\Gamma_j = \gamma_j G$. Les définitions et un raisonnement facile par récurrence nous conduisent aux inclusions suivantes:

$$\begin{array}{ccccccccc} 1 = Z_0 & \leqslant & Z_1 & \leqslant & \ldots, & & & & \\ \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} & & & & & & \\ 1 = G_0 & \leqslant & G_1 & \leqslant & \ldots & \leqslant & G_{s-1} & \leqslant & G_s = G, \\ & & & & & & \rotatebox{90}{$\leqslant$} & & \rotatebox{90}{$\leqslant$} \\ & & & & \ldots & \leqslant & \Gamma_2 & \leqslant & \Gamma_1 = G. \end{array} \tag{4}$$

On remarque que la série d'hypercentres et la série centrale dans le groupe nilpotent sont des matriochkas, i. e. contiennent 1 et G, et que le nombre des sections de chaque matriochka est égal au degré de nilpotence du groupe. Conformément au graphisme du diagramme (4), ces séries sont appelées *série centrale supérieure* et *série centrale inférieure* (le second terme a été formellement introduit encore dans le n° 14.4 mais sans explication). Bien que les matriochkas centrales supérieure et inférieure d'un groupe nilpotent ont même nombre de

termes, elles ne se confondent pas toujours (voir les exercices 16.2.10 et 16.2.11).

16.1.2. Exemple. Soient K un corps commutatif, $n \geqslant 3$. Utilisant les formules (9), (12) de l'exemple 3.2.1. IV, on voit sans peine que

$$\mathbf{UT}_n(K) = \mathbf{UT}_n^1(K) \geqslant \mathbf{UT}_n^2(K) \geqslant \ldots \geqslant \mathbf{UT}_n^n(K) = 1$$

est une matriochka centrale supérieure et inférieure à la fois dans le groupe $\mathbf{UT}_n(K)$. En particulier, c'est un groupe nilpotent de degré $n - 1$. Un des auteurs (voir You. I. Merzliakov, in: *Alguebra i loguika*, 1964, 3, n° 4, p. 49-58) a calculé les séries centrales d'autres groupes matriciels, notamment les séries centrales inférieures des sous-groupes de congruence principaux sur des anneaux locaux et celles des p-sous-groupes de Sylow dans $\mathbf{GL}_n(\mathbb{Z}_{p^m})$. Dans ce dernier cas, on a par exemple la description suivante. Désignons pour abréger $K = \mathbb{Z}_{p^m}$. Prenons une matrice vide d'ordre n, i. e. un carré partagé en n bandes horizontales et n bandes verticales, et recouvrons-la d'un *tapis d'idéaux* K, pK, p^2K, ... de la façon suivante (le schéma est tracé pour $n = 3$):

$$\begin{array}{ccccc|c|c|c|ccc}
\ldots p^2K & p^2K & p^2K & pK & pK & pK & K & K & K & & \\
\ldots p^2K & p^2K & p^2K & pK & & pK & pK & K & K & K & \\
\ldots \underbrace{p^2K \quad p^2K \quad p^2K}_{n} & & & & & \underbrace{pK \quad pK \quad pK}_{n} & & & \underbrace{K \quad K \quad K}_{n} & &
\end{array}$$

Soit G un p-sous-groupe de Sylow de $\mathbf{GL}_n(K)$. Nous savons qu'il réunit toutes les matrices d'ordre n sur K congrues à la matrice unité modulo le tapis d'idéaux dans la position montrée (exercice 11.3.3). Il se trouve que pour $r \geqslant 2$, le terme central $\gamma_r G$ contient uniquement les matrices de $\mathbf{SL}_n(K)$ congrues à l'unité modulo le tapis d'idéaux déplacé de $(r - 1)$ positions vers la droite. D'une façon plus formelle, soit K un anneau associatif unitaire. Son système d'idéaux $\mathfrak{a} = \{\mathfrak{a}_{ij} \mid i, j \in \mathbb{Z}\}$ s'appelle *tapis d'idéaux* si l'on a

$$\mathfrak{a}_{ik}\mathfrak{a}_{kj} \subseteq \mathfrak{a}_{ij} \quad \text{pour tous } i, j, k \in \mathbf{Z}.$$

On vérifie aisément que si K est commutatif, alors

$$\Gamma_n(\mathfrak{a}) = \{x \in \mathbf{SL}_n(K) \mid x_{ij} \equiv \delta_{ij} \bmod \mathfrak{a}_{ij}\}$$

est un groupe; il s'appelle *sous-groupe de congruence* (*spécial*) *modulo le tapis* $\mathfrak{a}$ (en particulier, pour $K = \mathbb{Z}$, $\mathfrak{a}_{ij} = (m)$ on retrouve $\Gamma_n(m)$ de l'exercice 4.2.7). Dans ces notations, le résultat précédent, traduit du langage des schémas en langage des formules, s'énonce

ainsi : si G est un p-sous-groupe de Sylow de $\mathrm{GL}_n(K)$ et $K = \mathbb{Z}_{p^m}$, on a

$$\gamma_r G = \Gamma_n(a^{(n,r)}), \quad r = 2, 3, \ldots,$$

où

$$a_{ij}^{(n,r)} = p^{-[(j-i-r)/n]}K;$$

les crochets signifient que l'on prend la partie entière et $p^l K = K$ pour $l \leqslant 0$. On voit en particulier qu'un p-sous-groupe de Sylow du groupe $\mathrm{GL}_n(\mathbb{Z}_{p^m})$ est nilpotent de degré $mn - 1$.

De la remarque qui suit la formule (4), il est clair qu'un groupe G est nilpotent de degré $\leqslant s$ si et seulement si $\gamma_{s+1}G = 1$. Aussi, la classe $\mathfrak{N}_s$ de tous les groupes nilpotents de degré $\leqslant s$ est-elle une variété définie par l'identité

$$\gamma_{s+1}(x_1, \ldots, x_{s+1}) \equiv [x_1, \ldots, x_{s+1}] = 1$$

(voir l'exercice 14.4.1). En particulier, $\mathfrak{N}_s$ est fermée pour la prise de sous-groupes, d'images homomorphes et de produits cartésiens. Conformément à la théorie générale développée dans le chapitre 5, la variété $\mathfrak{N}_s$ admet des groupes libres qui se laissent tous mettre sous la forme

$$\mathrm{F}(X)/\gamma_{s+1}\mathrm{F}(X),$$

où X est un alphabet convenable.

16.1.3. Exercice. Soit G un groupe libre nilpotent de degré 2 à générateurs libres a, b. Soit en outre $c = [b, a]$. Chaque élément g de G se laisse mettre d'une façon unique sous la forme $g = a^\alpha b^\beta c^\gamma$, α, β, γ entiers, et ceci en sorte que

$$a^\alpha b^\beta c^\gamma \cdot a^{\alpha'} b^{\beta'} c^{\gamma'} = a^{\alpha+\alpha'} b^{\beta+\beta'} c^{\gamma+\gamma'+\alpha'\beta}.$$

Par conséquent, l'application $a^\alpha b^\beta c^\gamma \mapsto \begin{pmatrix} 1 & \beta & \gamma \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}$ est un isomorphisme de G sur $\mathrm{UT}_3(\mathbb{Z})$.

Quelques mots sur la terminologie. Les groupes nilpotents n'ont pas reçu cette appellation dès le début : ils ont été longtemps désignés par le terme vague « groupes spéciaux », tandis que la notion de nilpotence était introduite depuis longtemps en théorie des anneaux : un anneau nilpotent, i.e. « nul en puissance », « potentiellement nul », est un anneau dans lequel le produit d'un nombre donné d'éléments quelconques est égal à zéro,

$$x_1 \ldots x_n = 0 \tag{5}$$

(tel est par exemple l'anneau des matrices trigonales d'ordre n à diagonale nulle). La théorie classique de Lie a établi une correspondance entre une classe d'anneaux — les anneaux de Lie — et une classe de groupes — les groupes de Lie — dans laquelle à la multiplication dans les anneaux correspond la commutation dans les groupes; en particulier, à l'identité (5) correspond l'identité

$$[x_1, \ldots, x_n] = 1. \tag{6}$$

Pour cette raison, le qualificatif « nilpotent » s'est appliqué finalement aussi aux groupes avec l'identité (6). Notons que la théorie des groupes n'est pas en reste avec la théorie des anneaux: c'est par analogie aux groupes résolubles que les anneaux de Lie résolubles ont été appelés.

Le lien entre la nilpotence des anneaux et celle des groupes est mis en relief une fois de plus par un

16.1.4. Exercice. Soit A un anneau associatif unitaire, soit B son sous-anneau quelconque, et soit B^n le sous-anneau engendré par les produits $b_1 \ldots b_n$, $b_i \in B$. Si le sous-anneau B est nilpotent, i.e. si $B^n = 0$ pour un certain n, les ensembles $G^{(i)} = \{1 - x \mid x \in B^i\}$ sont des groupes pour la multiplication dans A, avec $[G^{(i)}, G^{(j)}] \leqslant G^{(i+j)}$. En particulier, ils sont tous nilpotents de degré $\leqslant n$. Cela démontre, une fois de plus, la nilpotence de certains groupes de l'exemple 16.1.2 mais sans mentionner les matriochkas centrales.

16.1.5. Exercice. Dans tout groupe nilpotent sans torsion, l'unité est le seul élément qui soit le conjugué de son inverse.

16.1.6. Exercice. Tout groupe nilpotent périodique de type fini est fini.

Indication: utiliser l'exercice 14.3.2.

16.2. Propriétés générales. C'est la définition même d'un groupe nilpotent qui suggère une méthode claire et en général efficace d'étude des groupes nilpotents: la récurrence sur le degré de nilpotence. Dans cette méthode, on utilise le plus souvent les termes centraux et les hypercentres, mais aussi parfois d'autres sous-groupes. A ce titre, il est bon de considérer un

16.2.1. Lemme. *Soit G un groupe nilpotent de degré $s \geqslant 2$. Son sous-groupe quelconque engendré par le commutant et un élément de G est nilpotent de degré inférieur à s.*

Démonstration. Soient $a \in G$, $H = (a, [G, G])$. Puisque

$$[G, G] \leqslant (\zeta_{s-1}G) \cap H \leqslant \zeta_{s-1}H,$$

le groupe $H/\zeta_{s-1}H$ est cyclique. Puisque le groupe quotient par le centre ne peut être cyclique et distinct de 1, on a $\zeta_{s-1}H = H$, ce qu'il fallait démontrer.

Les propriétés des groupes nilpotents qui seront dégagées dans ce numéro se rapportent essentiellement aux sous-groupes.

16.2.2. Théorème. *Tout sous-groupe d'un groupe nilpotent est sous-normal. Plus exactement, si G est un groupe nilpotent de degré s, la suite des normalisateurs successifs de son sous-groupe quelconque H atteint G au bout de s pas tout au plus.*

Démonstration. Introduisons les notations

$$Z_i = \zeta_i G, \quad H_0 = H, \quad H_{j+1} = H_G(H_j).$$

Il suffit de vérifier que $Z_i \leqslant H_i$. Cela est évident pour $i = 0$. Passons de i à $i + 1$. Puisque

$$[G, Z_{i+1}] \leqslant Z_i \leqslant H_i,$$

on a

$$H^{Z_{i+1}} \leqslant H_i\,[H_i, Z_{i+1}] \leqslant H_i.$$

Cela revient à dire que Z_{i+1} normalise H_i, i.e. $Z_{i+1} \leqslant H_{i+1}$. Le théorème est démontré.

16.2.3. Théorème. *Dans un groupe nilpotent, tout sous-groupe normal non trivial admet une intersection non triviale avec le centre.*

Démonstration. Raisonnons par récurrence sur le degré de nilpotence. Soient G un groupe nilpotent, $H \trianglelefteq G$, $H \neq 1$, $Z_i = \zeta_i G$. Si $H \leqslant Z_1$, la proposition est triviale. Soit $H \not\leqslant Z_1$. Par hypothèse de récurrence appliquée à G/Z_1, l'intersection $HZ_1 \cap Z_2$ contient alors un élément $a \notin Z_1$. Puisque

$$a = hz, \quad h \in H, \quad z \in Z_1,$$

on a $h \in H \cap Z_2$, $h \notin Z_1$. Soit un $g \in G$ tel que $[h, g] \neq e$. On a alors

$$[h, g] \in H \cap [Z_2, G] \leqslant H \cap Z_1,$$

i.e. l'intersection $H \cap Z_1$ est non triviale. Le théorème est démontré.

16.2.4. Exercice. Dans un groupe nilpotent, tout sous-groupe normal d'ordre premier est contenu dans le centre.

16.2.5. Théorème. *Soit G un groupe nilpotent. Si A est son sous-groupe tel que $A\,[G, G] = G$, on a $A = G$. En particulier,*

$$[G, G] \leqslant \Phi(G). \tag{7}$$

Démonstration. Soit au contraire $A \neq G$. Posons $A_i = A \cdot \zeta_i G$, $i = 0, 1, 2, \ldots$ Il est évident que $A_i \trianglelefteq A_{i+1}$. Soient $A_m < G$, $A_{m+1} = G$. Puisque la section A_{m+1}/A_m est abélienne, on a $[G, G] \leqslant A_m$, d'où

$$A\,[G, G] \leqslant A_m < G.$$

On aboutit à une contradiction. L'assertion sur le sous-groupe de Frattini découle de sa définition en tant qu'ensemble d'éléments non générateurs (théorème 2.2.6). Le théorème est démontré.

[Dévoilons un secret. Dans les exemples de sous-groupes de Frattini 2.2.7, nous avions établi l'inclusion $\Phi(\mathbf{UT}_n(\mathbb{Z})) \leqslant \mathbf{UT}_n^2(\mathbb{Z})$ et remarqué que l'inclusion inverse est aussi valable (le soin de démontrer cette remarque étant laissé au lecteur !). Nous pensions justement au théorème 16.2.5.]

16.2.6. Théorème. *Dans un groupe nilpotent G, tout sous-groupe normal abélien maximal A se confond avec son centralisateur. En particulier, A est un sous-groupe abélien maximal et G/A admet une image isomorphe dans* Aut A.

Démonstration. Soient $H = C_G(A)$, $Z_i = \zeta_i G$. Supposons démontrée l'inclusion $H \cap Z_i \leqslant A$, et soit $x \in H \cap Z_{i+1}$. Pour tout $g \in G$ on a $[x, g] \in H \cap Z_i \leqslant A$, donc $\mathrm{gr}(x, A)$ est un sous-groupe normal abélien de G contenant A. Puisque A est maximal, on a $x \in A$, i. e. $H \cap Z_{i+1} \leqslant A$. Comme $Z_n = G$ pour un n déterminé, on a $H = A$, ce qu'il fallait démontrer.

Pour abréger, les éléments d'ordres finis seront appelés *éléments périodiques*.

16.2.7. Théorème. *Dans un groupe nilpotent G, l'ensemble τG des éléments périodiques (partie périodique de G) est un sous-groupe.*

Démonstration. Raisonnons par récurrence sur le degré de nilpotence et appliquons le lemme 16.2.1. Soient a, b deux éléments périodiques de G. Posons

$$A = (a, [G, G]), \quad B = (b, [G, G]).$$

Par hypothèse de récurrence, τA, τB sont sous-groupes de A, B respectivement. Puisque τA est End-permis dans A et que A est normal dans G, τA est normal dans G. Pour la même raison, τB est normal dans G. Puisque tout élément de $\tau A \cdot \tau B$, élevé à une puissance convenable, tombe d'abord dans τB et puis dans 1, le groupe $\tau A \cdot \tau B$ est périodique. En particulier, les éléments ab, a^{-1} sont périodiques, ce qu'il fallait démontrer.

16.2.8. Théorème. *Dans un groupe nilpotent G sans torsion, l'extraction de la racine est une opération univoque (sans être*

toujours définie partout), i.e. de $a^n = b^n$, $n \neq 0$, *il découle que* $a = b$.

Démonstration. Raisonnons par récurrence sur le degré de nilpotence. Le théorème étant évident pour les groupes abéliens, supposons que G soit non abélien. Considérons son sous-groupe $(a, [G, G])$. Il est normal dans G et nilpotent d'un degré moins grand que celui de G (lemme 16.2.1). Puisque $a, a^b \in (a, [G, G])$ et que, de toute évidence, $(a^b)^n = a^n$, on a par hypothèse de récurrence $a^b = a$. Il en découle que les éléments a et b commutent, d'où $(ab^{-1})^n = e$. Puisque G est sans torsion, on a $a = b$. Le théorème est démontré.

16.2.9. Exercice. Dans un groupe nilpotent sans torsion, $x^m y^n = y^n x^m$ $(m, n \neq 0) \Rightarrow xy = yx$.

Indication: $(y^{-n}xy^n)^m = x^m \Rightarrow y^{-n}xy^n = x$, etc.

16.2.10. Exercice. Dans les groupes nilpotents sans torsion, tous les facteurs de la série centrale supérieure sont sans torsion, eux aussi.

16.2.11. Exercice. Pour la série centrale inférieure la proposition précédente est fausse: par exemple, si

$$G = \begin{pmatrix} 1 & n\mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{on a} \quad [G, G] = \begin{pmatrix} 1 & 0 & n\mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

d'où $G/[G, G] \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_n$.

Considérons à présent les sous-groupes normaux nilpotents dans un groupe arbitraire.

16.2.12. Théorème (Fitting). *Dans un groupe quelconque, le produit de deux sous-groupes normaux nilpotents des degrés* s, t *est un sous-groupe normal nilpotent de degré* $\leqslant s + t$.

Démonstration. Soient $A \trianglelefteq G$, $B \trianglelefteq G$, $\gamma_{s+1}A = 1$, $\gamma_{t+1}B = 1$. On alors

$$\gamma_n(AB) = \underbrace{[AB, \ldots, AB]}_{n} = \prod [H_1, \ldots, H_n], \tag{8}$$

où chaque H_i se confond soit avec A, soit avec B (voir l'exercice 3.2.6). Puisque $\gamma_i A \overset{c}{\leqslant} A \trianglelefteq G$, on a $\gamma_i A \trianglelefteq G$ et donc

$$[\gamma_i A, B] \leqslant \gamma_i A \quad \text{pour tout } i.$$

Si donc i termes de $H_1, \ldots, H_n$ se confondent avec A et les $n - i$ autres avec B, on a

$$[H_1, \ldots, H_n] \leqslant \gamma_i A \cap \gamma_{n-i} B. \tag{9}$$

Prenons $n = s + t + 1$. On a alors soit $i \geqslant s + 1$, soit $n - i \geqslant t + 1$, d'où $\gamma_n(AB) = 1$ en vertu de (8), (9). Le théorème est démontré.

16.2.13. Exercice. Soit $\mathfrak{K}$ la classe de tous les groupes G tels que

$$\gamma_\omega G \equiv \bigcap_{n=1}^{\infty} \gamma_n G = 1.$$

Le produit de deux sous-groupes normaux appartenant à $\mathfrak{K}$ n'appartient pas forcément lui-même à $\mathfrak{K}$, un contre-exemple:

$$\mathrm{SL}_n(\mathbb{Z}) = \Gamma_n(2) \cdot \Gamma_n(3).$$

16.3. Groupes nilpotents d'automorphismes. Nous avons noté dans l'exemple 16.1.2 que tout groupe de matrices unitrigonales est nilpotent. Or, les matrices sont des automorphismes d'un espace vectoriel de base donnée, et les matrices unitrigonales sont exactement les automorphismes qui laissent inchangée la matriochka des sous-espaces engendrés par des segments finis décroissants de la base et opèrent identiquement dans les sections de cette matriochka. C'est cette propriété qui constitue la cause véritable de la nilpotence.

16.3.1. Lemme. *Soit donnée dans un groupe G une matriochka normale à $(r + 1)$ termes*

$$G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_r = 1; \tag{10}$$

soit Φ le groupe de tous les automorphismes du groupe G qui laissent invariants les termes de la matriochka (10) *et opèrent identiquement dans les sections G_i/G_{i+1} (le stabilisateur de la matriochka* (10)). *Considérons G, Φ comme des sous-groupes de l'holomorphe* Hol G. *Les groupes Φ et $[G, \Phi]$ sont nilpotents de degré $< r$.*

Démonstration. a) Le groupe Φ est nilpotent de degré $< r$. En effet, on a par définition

$$G_i^\Phi = G_i, \quad [G_i, \Phi] \leqslant G_{i+1} \text{ pour tout } i. \tag{11}$$

Soit Φ_j centralisateur dans Φ des sections G_i/G_{i+j}, $i = 0, 1, 2, \ldots$ Il est évident que

$$\Phi = \Phi_1 \geqslant \Phi_2 \geqslant \ldots \geqslant \Phi_r = 1;$$

il suffit donc de montrer que c'est une matriochka centrale dans Φ, i.e.

$$[\Phi_j, \Phi] \leqslant \Phi_{j+1} \quad \text{pour tout } j$$

ou

$$[G_i, [\Phi_j, \Phi]] \leqslant G_{i+j+1} \text{ pour tous } i, j.$$

Or, cela ressort des relations

$$[\Phi_j, [\Phi, G_i]] \leqslant [\Phi_j, G_{i+1}] \leqslant G_{i+j+1},$$
$$[\Phi, [G_i, \Phi_j]] \leqslant [\Phi, G_{i+j}] \leqslant G_{i+j+1}$$

en vertu du lemme des trois commutants 3.2.3.

b) Le groupe $[G, \Phi]$ est nilpotent de degré $< r$. En effet,

$$[G, [\Phi, G_i]] \leqslant [G, G_{i+1}] \leqslant G_{i+1},$$
$$[\Phi, [G_i, G]] \leqslant [\Phi, G_i] \leqslant G_{i+1},$$

d'où comme précédemment, en vertu du lemme des trois commutants,

$$[G_i, [G, \Phi]] \leqslant G_{i+1} \quad \text{pour tout } i.$$

Cela revient à dire que les conjugaisons par éléments de $[G, \Phi]$ opèrent identiquement dans les sections de la matriochka $G_1 \geqslant G_2 \geqslant \geqslant \ldots \geqslant G_r = 1$. D'après la proposition a) démontrée ci-dessus, le groupe de ces conjugaisons, i.e.

$$[G, \Phi]/C_{[G, \Phi]}(G_1),$$

est nilpotent de degré $< r - 1$. Or, $[G, \Phi] \leqslant G_1$, aussi $C_{[G, \Phi]}(G_1)$ est-il contenu dans le centre de $[G, \Phi]$, d'où la proposition b). Le lemme est démontré.

Il est naturel d'aller plus loin et de se demander si le stabilisateur d'une matriochka de sous-groupes quelconque (pas forcément normale) est nilpotent. Par stabilisateur de la matriochka (10), on entend ici le sous-groupe maximal Φ de Aut G vérifiant la condition (11). Il se trouve que la réponse est positive comme précédemment, bien que la démonstration soit plus compliquée et que l'évaluation du degré de nilpotence soit moins bonne:

16.3.2. Théorème (Ph. Hall). *Le stabilisateur d'une matriochka de sous-groupes quelconque à $(r+1)$ termes est un groupe nilpotent de degré $\leqslant \binom{r}{2}$.*

Démonstration. Raisonnons par récurrence sur r. Soit Φ stabilisateur de la matriochka (10). Soit en outre $\Psi = C_\Phi(G_1)$. Puisque Φ stabilise la matriochka à r termes $G_1 \geqslant G_2 \geqslant \ldots$, par hypothèse de récurrence le groupe Φ/Ψ est nilpotent de degré $\leqslant \binom{r-1}{2}$

$$\gamma_{1+\binom{r-1}{2}}\Phi \leqslant \Psi.$$

Désignons

$$\Psi_1 = \Psi, \quad \Psi_{i+1} = [\Psi_i, \Phi].$$

Puisque $\Psi \trianglelefteq \Phi$, on a $\Psi = \Psi_1 \geqslant \Psi_2 \geqslant \ldots$ Il suffit de montrer que $[G, \Psi_r] = 1$. A cet effet, vérifions que $[G, \Psi_i] \leqslant G_i$ pour tout i.

Cela est évident pour $i = 1$. Passons de i à $i + 1$. Soient $g \in G$, $\psi_{i+1} \in \Psi_{i+1}$. Il s'agit de montrer que $[\psi_{i+1}, g] \in G_{i+1}$. Or, ψ_{i+1} est un mot construit sur des commutateurs de la forme

$$[\psi_i, \varphi^{-1}], \quad \psi_i \in \Psi_i, \quad \varphi \in \Phi.$$

L'élément $\psi_i^g{}_1$ est le même mot construit sur les produits

$$[\psi_i, \varphi^{-1}]^g = [\psi_i, \varphi^{-1}]\,[\psi_i, \varphi^{-1}, g]. \tag{12}$$

Remarquons que

$$[\psi_i, \varphi^{-1}, g] \in G_{i+1}$$

en vertu de l'identité de Ph. Hall (voir la formule (16) dans le lemme 3.2.3) et des relations

$$[\varphi, g^{-1}, \psi_i] \in [\Phi, G, \Psi_i] \leqslant [G_1, \Psi] = 1,$$
$$[g, \psi_i^{-1}, \varphi] \in [G, \Psi_i, \Phi] \leqslant [G_i, \Phi] \leqslant G_{i+1}.$$

Donc, le facteur de gauche dans (12) appartient à Ψ et le facteur de droite à G_{i+1}. Or, Ψ centralise $G_1 \geqslant G_{i+1}$, d'où $\psi_{i+1}^g \in \psi_{i+1} G_{i+1}$. Par suite, $[\psi_{i+1}, g] \in G_{i+1}$, et le théorème est démontré.

L'exemple 16.1.2 nous aura mené bien loin!

§ 17. Quelques sous-classes importantes

17.1 Groupes nilpotents finis. Nous allons décrire une autre source importante de groupes nilpotents.

17.1.1. Exemple. Tout p-groupe fini G est nilpotent. En effet, G admet un centre non trivial. Pour le démontrer, remarquons qu'un élément est central si et seulement s'il forme une classe de conjugaison complète. Puisque

$$|a^G| = |G : N_G(a)|,$$

les cardinaux c_i des classes de conjugaison dans G sont des puissances de p. Puisque l'unité est une classe de conjugaison complète, il existe au moins un c_i égal à 1. Or, leur somme $\sum c_i = |G|$ est divisible par p, c'est pourquoi il existe plusieurs autres c_i égaux à 1. Ainsi donc, G a un centre non trivial Z_1. Pour la même raison, G/Z_1 a un centre non trivial Z_2/Z_1, etc. Nous voyons qu'un hypercentre assez grand du groupe G se confond avec G tout entier: cela veut dire que G est nilpotent.

17.1.2. Exercice. Soit p un nombre premier. Il n'existe que deux groupes d'ordre p^2 non isomorphes: $\mathbb{Z}_{p^2}$ et $\mathbb{Z}_p \times \mathbb{Z}_p$. Il existe cinq groupes d'ordre p^3: trois groupes abéliens

$$\mathbb{Z}_{p^3}, \quad \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$$

et deux groupes non abéliens. Pour $p = 2$, ce sont le groupe diédral

$$\mathrm{gr}\,(a,\ b \parallel a^4 = 1,\quad b^2 = 1,\quad bab = a^{-1})$$

et le groupe quaternionien

$$\mathrm{gr}\,(a,\ b \parallel a^4 = 1,\quad b^2 = a^2,\quad b^{-1}ab = a^{-1}),$$

et pour $p > 2$

$$\mathrm{gr}\,(a,\ b \parallel a^{p^2} = 1,\ b^p = 1,\quad b^{-1}ab = a^{1+p}),$$

$$\mathrm{gr}\,(a,\ b,\ c \parallel a^p = 1,\quad b^p = 1,\quad c^p = 1,$$
$$[a,\ b] = c,\quad [a,\ c] = [b,\ c] = 1).$$

Il existe des p-groupes infinis non nilpotents: par exemple, l'entrelacement direct d'un p-groupe non trivial avec un p-groupe infini est un p-groupe sans centre (voir l'exercice 6.2.3). Un exemple concret: $\mathbf{C}_{p^\infty} \wr \mathbf{C}_{p^\infty}$. Un autre procédé utile pour obtenir un groupe sans centre consiste à déplacer celui-ci d'une façon constante en l'agrandissant:

17.1.3. Exercice. Soient K un corps commutatif de caractéristique p strictement positive, et $\mathbf{UT}_\omega\,(K)$ un groupe de matrices infinies sur K dans lesquelles les lignes et les colonnes sont numérotées par des entiers naturels, tous les éléments diagonaux sont égaux à 1, les éléments sous la diagonale sont tous nuls, et les éléments au-dessus de la diagonale, nuls à l'exception d'un nombre fini d'éléments. Le groupe $\mathbf{UT}_\omega\,(K)$ est un p-groupe sans centre (voir la formule (2) de l'exemple 3.1.1. IV).

Il se trouve que tout groupe nilpotent fini est produit direct d'un nombre fini de p-groupes finis. On peut faire mieux et démontrer un

17.1.4. Théorème (Burnside-Wielandt). *Soit G un groupe fini. Les conditions suivantes sont équivalentes:*

a) *G est nilpotent,*

b) *tout sous-groupe de G est sous-normal,*

c) *G est produit direct de ses p-sous-groupes de Sylow,*

d) $[G,\ G] \leqslant \Phi\,(G)$.

Démonstration. Procédons dans l'ordre conforme au diagramme suivant:

$$\begin{tikzcd}
 & \mathrm{a)} \arrow[dl, shift left] \arrow[dr, shift left] & \\
\mathrm{b)} \arrow[dr, shift left] & & \mathrm{d)} \arrow[ul, shift left] \arrow[dl, shift left] \\
 & \mathrm{c)} \arrow[uu, Rightarrow] &
\end{tikzcd}$$

a) $\Rightarrow$ b). Voir le théorème 16.2.2.

b) $\Rightarrow$ c). Soit P un p-sous-groupe de Sylow dans G. Puisque $N_G(P)$ se confond avec son normalisateur dans G (exercice 11.1.4) et qu'en vertu de b) le normalisateur de tout sous-groupe propre est plus grand que le sous-groupe lui-même, on a $N_G(P) = G$. Ainsi donc, les p-sous-groupes de Sylow sont normaux dans G, d'où l'on déduit sans peine la condition c).

c) $\Rightarrow$ a). Voir l'exemple 17.1.1.

a) $\Rightarrow$ d). Voir le théorème 16.2.5.

d) $\Rightarrow$ c). Ici encore, il suffit de vérifier que tout p-sous-groupe de Sylow P du groupe G est normal dans G. Supposons par absurde que $N_G(P)$ soit un sous-groupe propre dans G, et H un sous-groupe maximal de G qui contient $N_G(P)$. Puisque

$$[G, G] \leqslant \Phi(G) \leqslant H,$$

H est normal dans G. D'autre part, H contient $N_G(P)$ et doit donc se confondre avec son normalisateur dans G (exercice 11.1.4). La contradiction obtenue achève la démonstration du théorème.

Du théorème de Burnside-Wielandt il ressort immédiatement que l'entrelacement d'un p-groupe fini non trivial avec un q-groupe fini non trivial est nilpotent si et seulement si $p = q$.

17.1.5. Exercice. Quel est le degré de nilpotence de l'entrelacement $\mathbb{Z}_{p^m} \wr \mathbb{Z}_p$?

La question de savoir sous quelles conditions un entrelacement est nilpotent reçoit une réponse exhaustive dans l'exercice suivant.

17.1.6. Exercice. Soient A, B deux groupes nilpotents non triviaux. Chacun des entrelacements $A \wr B$, $A \bar{\wr} B$ est nilpotent si et seulement si A et B sont des p-groupes, B étant fini et A de période finie.

Indication. Utiliser les exercices 6.2.1, 6.2.3. et faire intervenir l'homomorphisme canonique $\mathbb{Z} \wr \mathbb{Z}_p \to \mathbb{Z}_q \wr \mathbb{Z}_p$.

Avant de terminer ce n°, citons un résultat relatif à des groupes finis arbitraires:

17.1.7. Théorème (Frattini). *Le sous-groupe de Frattini d'un groupe fini est nilpotent.*

Démonstration. Soient G un groupe fini et A son sous-groupe de Frattini. En vertu du théorème 17.1.4, il suffit de vérifier que tout p-sous-groupe de Sylow P du groupe A est normal dans A ou, ce qui revient au même, dans G (voir l'exercice 5.2.6), i. e. $N_G(P) = G$. Or, cela équivaut à la relation

$$G = A \cdot N_G(P),$$

car A est un ensemble fini d'éléments non générateurs du groupe G (théorème 2.2.6). C'est cette dernière relation que nous nous appliquerons à démontrer.

Soit g un élément quelconque de G. En conjuguant G par g, on obtient une application de A dans lui-même, aussi P^g est-il encore un p-sous-groupe de Sylow de A. En vertu du théorème de Sylow 11.1.1, les sous-groupes P et P^g sont conjugués par un élément $a \in A$, i.e. $P^g = P^a$. D'où $ga^{-1} \in N_G(P)$, $g \in A \cdot N_G(P)$. Le théorème est démontré.

Notons que nous venons de démontrer en passant un

17.1.8. Lemme (Frattini). *Soient A un sous-groupe normal d'un groupe fini G, et P son p-sous-groupe de Sylow. On a $G = A \cdot N_G(P)$.*

17.1.9. Exercice. Soient A un sous-groupe normal d'un groupe G, et B un sous-groupe de A tel que $B, B' \leqslant A$ soient conjugués dans A si et seulement si B, B' le sont aussi dans G. Dans ce cas, $G = A \cdot N_G(B)$. (Lemme de Frattini généralisé.)

17.2. Groupes nilpotents de type fini. Un exemple évident de tels groupes est $\mathbf{UT}_n(\mathbb{Z})$. Il se trouve que les sous-groupes d'un groupe unitrigonal sur $\mathbb{Z}$ sont les seuls groupes nilpotents de type fini sans torsion; quant aux groupes nilpotents quelconques de type fini, chacun d'eux est une extension finie d'un groupe sans torsion et, en particulier, se plonge dans $\mathbf{SL}_n(\mathbb{Z})$. Nous établirons ici ces deux faits capitaux en théorie des groupes nilpotents de type fini.

17.2.1. Lemme. *Soit G un groupe quelconque. Si G est engendré par un ensemble M, son terme central $\gamma_i G$ est engendré par le terme central suivant $\gamma_{i+1}G$ et des commutateurs simples de poids i en éléments de M.*

Démonstration. Pour $i = 1$, la proposition est évidente. Passons de i à $i + 1$. Par définition, $\gamma_{i+1}G$ est engendré par les éléments $[x, y]$, $x \in \gamma_i G$, $y \in G$. Par hypothèse de récurrence, $x = x_1^{\varepsilon_1} \ldots x_m^{\varepsilon_m} z$, où chaque x_j est un commutateur simple de poids i en éléments de M, $z \in \gamma_{i+1}G$, $\varepsilon_j = \pm 1$. Ensuite, y est un mot en éléments de $M \cup M^{-1}$. Utilisant les relations entre commutateurs (3) du n° 3.2, nous remarquons que $[x, y]$ est un mot en éléments de la forme

$$[x_j, a]^g = [x_j, a]\,[x_j, a, g],\ [z, a]^g,$$
$$a \in M, \quad g \in G.$$

Puisque $[x_j, a, g]$, $[z, a]$ appartiennent à $\gamma_{i+2}G$, le lemme est démontré.

Nous disons que le groupe *possède presque* une propriété donnée s'il contient un sous-groupe normal d'indice fini qui possède la propriété en question.

17.2.2. Théorème. *Tout groupe nilpotent de type fini G admet une matriochka centrale à sections cycliques et est presque sans torsion. Si G est absolument sans torsion, il admet une matriochka centrale à sections cycliques infinies.*

Démonstration. a) Soit G de type fini et nilpotent. Chaque section de sa matriochka centrale inférieure est un groupe abélien de type fini (voir lemme 17.2.1) et, à ce titre, admet une matriochka à sections cycliques. Puisque toute subdivision d'une matriochka centrale est encore une matriochka centrale, G admet une matriochka centrale à sections cycliques. Par récurrence sur le nombre des termes de la matriochka, montrons que G est presque sans torsion. Soit H le plus grand terme de la matriochka distinct de G; soit a un élément générateur de G (mod H). Par hypothèse de récurrence, H est presque sans torsion; il existe donc un m tel que le sous-groupe $H^m = (h^m \mid h \in H)$ soit sans torsion. Conformément à l'exercice 16.1.6, on a $|H : H^m| < \infty$. Si $|G : H| < \infty$, alors H^m est le sous-groupe sans torsion cherché dans G. Soit $|G : H| = \infty$. Alors $(a)\, H^m$ contient le sous-groupe cherché, car il est sans torsion et

$$|G : (a)\, H^m| = |H : H \cap (a)\, H^m| \leqslant |H : H^m| < \infty.$$

b) Soit G un groupe nilpotent sans torsion. Nous venons de voir qu'il est polycyclique, c'est pourquoi les sections de sa matriochka centrale supérieure sont polycycliques, elles aussi (exercice 4.4.3). Puisque ce sont des groupes sans torsion (exercice 16.2.10), la matriochka centrale supérieure peut être subdivisée de façon à posséder des sections cycliques infinies. Le théorème est démontré.

17.2.3. Exercice. Tout groupe polycyclique est presque sans torsion.

Indication: voir la démonstration du théorème 17.2.2.

17.2.4. Exercice. La partie périodique de tout groupe nilpotent de type fini est finie. D'une façon plus générale, si le groupe est presque sans torsion, ses sous-groupes périodiques sont finis.

Grâce au théorème 17.2.2, un groupe nilpotent de type fini sans torsion G peut être muni de coordonnées entières d'un type particulier qui permettent de représenter G par des matrices unitrigonales entières. Plus exactement, soit G un ensemble. Une famille de fonctions $f_i : G \to \mathbb{Z}$, $i = 1, \ldots, s$, s'appelle *famille de coordonnées* si l'application $x \mapsto (f_1(x), \ldots, f_s(x))$ est une injection

de G dans l'ensemble $\mathbb{Z}^s$ de tous les s-uplets entiers. Soit $G \subseteq \mathbb{Z}^s$. L'application φ: $G \to \mathbb{Z}^r$ est dite *polynomiale* s'il existe des polynômes $f_1, \ldots, f_r$ de s variables à coefficients dans $\mathbb{Q}$, tels que

$$x^\varphi = (f_1(x), \ldots, f_r(x)) \text{ pour } x \in G.$$

Si $f_1, \ldots, f_r$ sont des polynômes du premier degré, on dit que φ est une *application linéaire*. Soit maintenant G un groupe nilpotent de type fini sans torsion. Considérons sa matriochka centrale

$$G = G_1 > G_2 > \ldots > G_{s+1} = 1$$

à sections cycliques infinies et choisissons des éléments $a_1, \ldots, a_s$ tels que $G_i = \mathrm{gr}\,(a_i, G_{i+1})$. Il est évident que chaque élément x de G se laisse mettre d'une façon unique sous la forme

$$x = a_1^{t_1(x)} \ldots a_s^{t_s(x)}, \qquad t_i(x) \in \mathbb{Z},$$

si bien que les fonctions $t_1, \ldots, t_s$ forment une famille de coordonnées. Le système ordonné $a_1, \ldots, a_s$ sera appelé *base de Maltsev* du groupe G, et les nombres $t_1(x), \ldots, t_s(x)$, les *coordonnées* de l'élément x dans cette base.

17.2.5. Théorème. *Soit G un groupe nilpotent de type fini sans torsion muni de coordonnées de Maltsev $t_1, \ldots, t_s$. Il existe un entier naturel $n = n(G)$ et un homomorphisme injectif $\varphi: G \to \mathrm{UT}_n(\mathbb{Z})$ tels que l'application φ soit polynomiale sur G et que son inverse φ^{-1} soit linéaire sur G^φ (en coordonnées matricielles introduites sur $\mathrm{UT}_n(\mathbb{Z})$). En particulier, la multiplication et l'élévation à une puissance dans le groupe G s'écrivent par des polynômes en coordonnées de Maltsev. Plus exactement, si $x, y \in G$, $m \in \mathbb{Z}$, $1 \leqslant i \leqslant s$, alors $t_i(xy)$ est un polynôme sur $\mathbb{Q}$*

$$\text{en } \{t_\alpha(x), t_\alpha(y) \mid \alpha < i\} + t_i(x) + t_i(y), \tag{1}$$

$t_i(x^m)$ est un polynôme sur $\mathbb{Q}$

$$\text{en } m \text{ et } \{t_\alpha(x) \mid \alpha < i\} + m t_i(x). \tag{2}$$

Démonstration. a) Démontrons d'abord ce que nous venons d'affirmer « en particulier ». Pour toute matrice a de $\mathrm{UT}_n(\mathbb{Z})$ et pour tout m de $\mathbb{Z}$ on a

$$a^m = \sum_{i=0}^{n-1} \binom{m}{i} (a-e)^i,$$

où

$$\binom{m}{i} = \frac{m(m-1)\ldots(m-i+1)}{i!}, \qquad \binom{m}{0} = 1, \tag{3}$$

i. e. les coefficients de la matrice a^m sont des polynômes en m et en coefficients de la matrice a. En vertu de la proposition principale du théorème, les coordonnées $t_i(xy)$, $t_i(x^m)$ se laissent exprimer de façon linéaire en fonction des coefficients des matrices $(xy)^\varphi$, $(x^m)^\varphi$ qui se laissent exprimer de façon polynomiale en fonction des coefficients des matrices x^φ, y^φ et du nombre m. Toujours en vertu de la proposition principale du théorème, les coefficients des matrices x^φ, y^φ se laissent exprimer de façon polynomiale en fonction des coordonnées $t_\alpha(x)$, $t_\alpha(y)$, aussi les coordonnées de Maltsev du produit xy et de la puissance x^m d'éléments sont-elles des polynômes en coordonnées de Maltsev des éléments x, y et du nombre m. Le fait que ces polynômes se laissent mettre sous la forme (1), (2) ressort immédiatement de la définition d'une matriochka centrale.

b) Remarquons maintenant qu'au lieu de l'injection φ, il suffit d'indiquer une injection polynomiale $\psi: G \to \mathbf{GL}_n(\mathbb{Z})$ telle que son inverse ψ^{-1} soit linéaire sur G^ψ, ce dernier ensemble étant constitué de matrices unipotentes (une matrice a est dite *unipotente* si elle admet une racine caractéristique unique 1 ou, ce qui revient au même, si $(a - e)^n = 0$). En effet, le groupe $H = G^\psi$ peut être appliqué dans $\mathbf{UT}_n(\mathbb{Z})$ par conjugaison dans $\mathbf{GL}_n(\mathbb{Q})$. Nous montrerons d'abord que H est le conjugué d'un sous-groupe de $\mathbf{UT}_n(\mathbb{Q})$. Assimilons $\mathbf{GL}_n(\mathbb{Q})$ au groupe des automorphismes d'un espace vectoriel V à n dimensions sur le corps $\mathbb{Q}$ et considérons une matriochka non subdivisible $V = V_1 > V_2 > \ldots > V_{m+1} = 0$ de sous-espaces invariants par H. Dans la base associée à cette matriochka, les automorphismes de H se mettent sous la forme de matrices trigonales par blocs dont les blocs diagonaux représentent l'action de H dans les sections V_i/V_{i+1}; il suffit donc de montrer que chaque section U de ce type est de dimension 1. Puisque le commutant $[H, H]$ est nilpotent d'un degré inférieur, on peut admettre que $[H, H]$ se laisse mettre sous la forme unitrigonale. Il existe alors un vecteur non nul $u \in U$ fixe pour tout automorphisme de $[H, H]$. Soit U' le sous-espace formé par tous les vecteurs de ce type. Il est invariant par H, car pour $h \in H$, $h' \in [H, H]$ on a

$$(uh)\, h' = u\,(hh'h^{-1})\, h = uh.$$

Puisque la section U ne contient aucun sous-espace propre invariant par H, on a $U' = U$, d'où $[H, H] = 1$ sur U; autrement dit, H induit un groupe abélien d'automorphismes de la section U. Or, tout ensemble de transformations linéaires permutables admet un vecteur propre commun sur l'extension du corps de base obtenue par les racines caractéristiques de ces transformations. Puisque le groupe H est unipotent, il admet un vecteur propre commun dans U. Comme le sous-espace engendré par ce vecteur est invariant par H, et U ne contient aucun sous-espace propre invariant, la dimension de U est 1. Cela revient à dire que $H^a \leqslant \mathbf{UT}_n(\mathbb{Q})$ pour un a convena-

blement choisi dans $\mathrm{GL}_n(\mathbb{Q})$. Considérons maintenant dans H^a une famille finie de matrices génératrices. Soient N le dénominateur commun de leurs coefficients et b une matrice telle que

$$b = \operatorname{diag}(1, N, N^2, \ldots, N^{n-1}).$$

Il est facile de voir que $H^{ab} \leqslant \mathrm{UT}_n(\mathbb{Z})$.

c) Il reste à démontrer l'existence de ψ. Nous le ferons par récurrence sur la longueur de la base de Maltsev. Supposons que, pour les groupes dont la base de Maltsev a une longueur inférieure à s, la représentation matricielle cherchée soit déjà trouvée, ce qui revient à dire que le théorème est démontré dans sa totalité (voir a), b)). Soit G un groupe muni d'une base de Maltsev $a_1, \ldots, a_s$ de longueur s. Avant de passer à la construction de ψ, nous établirons dans ce n° la formule (1) pour le groupe G. Désignons abréviativement $t_i(x) = \xi_i$, $t_i(y) = \eta_i$. Il est évident que

$$xy = a_1^{\xi_1+\eta_1}(a_1^{-\eta_1}a_2^{-1}a_1^{\eta_1})^{-\xi_2} \ldots (a_1^{-\eta_1}a_s^{-1}a_1^{\eta_1})^{-\xi_s}a_2^{\eta_2} \ldots a_s^{\eta_s}$$

et

$$a_1^{-\eta}a_i^{-1}a_1^{\eta} = [a_1^{\eta}, a_i]\, a_i^{-1}.$$

Par hypothèse de récurrence et en vertu de a), b), les formules (1), (2) restent valables pour les groupes dont la base de Maltsev a une longueur inférieure à s; il suffit donc de vérifier que les coordonnées des éléments $[a_1^{\eta}, a_i]$ dans la base de Maltsev $a_2, \ldots, a_s$ sont des polynômes en η. Il est évident que

$$[a_1^{\eta}, a_i] = a_1^{-\eta}(a_i^{-1}a_1a_i)^{\eta}$$

et

$$a_i^{-1}a_1a_i = a_1a_{i+1}^{c_{i,\,i+1}} \ldots a_s^{c_{is}}, \quad c_{ij} \in \mathbb{Z}.$$

Par hypothèse de récurrence appliquée à gr $(a_1, a_{i+1}, \ldots, a_s)$, on obtient

$$(a_i^{-1}a_1a_i)^{\eta} = a_1^{\eta}a_{i+1}^{\zeta_{i,\,i+1}} \ldots a_s^{\zeta_{is}},$$

où ζ_{is} sont des polynômes en η. D'où $[a_1^{\eta}, a_i] = a_{i+1}^{\zeta_{i,\,i+1}} \ldots a_s^{\zeta_{is}}$, et la formule (1) est démontrée pour le groupe G.

d) Passons à la construction e ψ. Soit $\mathbb{Q}[t]$ l'anneau des polynômes sur $\mathbb{Q}$ en fonctions $t_1, \ldots, t_s$. Définissons l'action de G sur cet anneau en posant que pour tout a de G

$$f^a(x) = f(ax), \quad f \in \mathbb{Q}[t], \quad x \in G$$

(« translation à gauche de l'argument »). On vérifie immédiatement que l'opérateur op (a) défini par cette formule est un automorphisme

de l'anneau $\mathbb{Q}[t]$ et que la loi $a \mapsto \mathrm{op}(a)$ définit un isomorphisme $G \to \mathrm{Aut}(\mathbb{Q}[t])$.

Un produit de la forme $M(t) = t_1^{m_1} \ldots t_s^{m_s}$ s'appelle *monôme* en $t_1, \ldots, t_s$. En vertu de (1)

$$t_i^a = t_i + \sum_j c_{ij}(a) M_j(t), \tag{4}$$

où $c_{ij}(a)$ est un polynôme sur $\mathbb{Q}$ en coordonnées de Maltsev de l'élément a, tandis que les monômes $M_j(t)$ intervenant avec des coefficients non nuls dans l'expression de t_i^a ne contiennent pas les variables $t_i, \ldots, t_s$. On voit de là que $\mathrm{op}(a) - \mathrm{op}(e)$ associe à un monôme quelconque $M(t)$ soit 0, soit une combinaison linéaire de monômes plus petits, les monômes étant ordonnés suivant leurs derniers exposants. La transformation $(\mathrm{op}(a) - \mathrm{op}(e))^m$ annule donc $M(t)$ pour un certain $m = m(a, M)$.

Soit H le sous-groupe additif engendré par l'orbite de l'ensemble des fonctions coordonnées $\{t_1, \ldots, t_s\}$ par rapport aux opérateurs $\mathrm{op}(x)$, $x \in G$. En vertu de (4), H est contenu dans le sous-groupe engendré par les fonctions $\left\{t_i, \frac{1}{N} M_j(t)\right\}$ pour un N naturel, ce qui signifie que H est un groupe de type fini. Soit $h_1, \ldots, h_n$ une base dans le groupe abélien libre H. Soit encore

$$h_k^x = \sum_l \psi_{kl}(x) h_l, \tag{5}$$

i.e. $(\psi_{kl}(x))$ est la matrice de la restriction de $\mathrm{op}(x)$ à H dans la base $h_1, \ldots, h_n$. Puisque H contient les fonctions coordonnées $t_1, \ldots, t_s$, la loi $x \mapsto (\psi_{kl}(x))$ définit un isomorphisme $\psi: G \to \mathrm{GL}_n(\mathbb{Z})$, le groupe G^ψ étant constitué de matrices unipotentes. L'application ψ^{-1} est linéaire sur G^ψ, car l'ensemble $\{t_i\}$ se laisse définir de façon linéaire en fonction de $\{h_k\}$, tandis que, en calculant les fonctions (5) au point e, nous voyons que $\{h_k\}$ se laisse définir de façon linéaire en fonction de $\{\psi_{kl}\}$. L'application ψ elle-même est polynomiale, i.e. les fonctions ψ_{kl} sont des restrictions à G de certains polynômes sur $\mathbb{Q}$. En effet, soit $x \in G$. Puisque chaque h_k est une combinaison linéaire sur $\mathbb{Z}$ de certains t_i^g, $g \in G$, on conçoit que h_k^x est, en vertu de (4), une combinaison analogue de

$$t_i^{gx} = t_i + \sum_j c_{ij}(gx) M_j(t).$$

D'où

$$h_k^x = \sum_j P_{kj}(x) M_j(t), \tag{6}$$

où P_{kj} est un polynôme sur $\mathbb{Q}$; en particulier,

$$h_k = \sum_j P_{kj}(e) M_j(t). \tag{7}$$

Puisque l'ensemble $\{h_k\}$ est linéairement indépendant sur $\mathbb{Q}$, les lignes de la matrice $(P_{kj}(e))$ le sont aussi. Portant (6), (7) dans (5) et profitant de l'indépendance linéaire de $\{M_j(t)\}$, on obtient un système d'équations linéaires pour $\psi_{kl}(x)$:

$$P_{kj}(x) = \sum_l \psi_{kl}(x) P_{lj}(e),$$

ce qui montre justement que les fonctions ψ_{kl} sont polynomiales sur $\mathbb{Q}$. Le théorème est démontré.

A propos de la démonstration que nous venons de développer, signalons qu'il existe une méthode générale permettant d'établir la représentabilité isomorphe des groupes par des matrices, dite *méthode de séparation des coordonnées* (Iou. I. Merzliakov in : *Alguebra i loguika*, 1968, 7, n° 3, p. 63-104). Cette méthode est exposée aussi dans [25].

17.2.6. Exercice. Soit p un nombre premier. Tout groupe nilpotent de type fini sans torsion admet une approximation par des p-groupes finis.

Indication: voir la démonstration du théorème 14.2.2.

Au commencement de ce n°, nous avons dit que les théorèmes 17.2.2 et 17.2.5 permettent de conclure que tout groupe nilpotent de type fini G se plonge dans $\mathbf{SL}_n(\mathbb{Z})$ pour un n déterminé. Il suffit de toute évidence d'indiquer une injection $\varphi: G \to \mathbf{GL}_m(\mathbb{Z})$, car $x \mapsto \begin{pmatrix} x^\varphi & 0 \\ 0 & x^\varphi \end{pmatrix}$ sera alors l'injection cherchée. Il reste à formuler une remarque générale. Soit H un sous-groupe d'indice fini m dans un groupe arbitraire G. Soient $a_1, \ldots, a_m$ les représentants des classes à droite de G suivant H. Si σ est une représentation fidèle de H par des matrices d'ordre n, la formule

$$g \mapsto \| (a_i g a_j^{-1})^\sigma \|$$

définit une représentation fidèle de G par des matrices d'ordre mn (on pose $x^\sigma = 0$ pour $x \notin H$). Evidemment, ce n'est autre que la représentation de G induite par σ (voir le n° 12.2).

17.2.7. Exercice. Un groupe qui est presque représentable par des matrices sur un anneau unitaire est complètement représentable par des matrices sur cet anneau.

17.2.8. Exercice. Tout groupe nilpotent de type fini est résiduellement fini.

17.2.9. Exercice. Il existe des groupes nilpotents de type fini sans torsion A, B qui peuvent être injectés l'un dans l'autre par des homomorphismes sans être isomorphes, par exemple:

$$=\begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}, \quad B=\begin{pmatrix} 1 & n\mathbb{Z} & \mathbb{Z} \\ 0 & 0 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix} \text{ pour } n \neq 0,\ 1.$$

17.2.10. Exercice. Un groupe nilpotent de type fini qui possède un centre fini est fini lui-même.

17.3. Groupes nilpotents sans torsion. Dans cette classe de groupes, un intérêt particulier est présenté par la théorie de l'extraction de la racine, qui sera exposée dans ce n°. Son point de départ est le théorème 16.2.8 selon lequel dans tout groupe nilpotent sans torsion G l'extraction de la racine est une opération partielle, i.e. univoque mais pas toujours définie partout. Il se trouve que G peut toujours être plongé dans un groupe nilpotent complet (où l'extraction de la racine est partout définie) et que deux complétés nilpotents « minimaux » quelconques de G sont isomorphes entre eux et se réduisent entièrement aux racines des éléments de G.

Rappelons qu'un groupe arbitraire G est dit *complet* si, pour l'un quelconque de ses éléments g et pour tout entier naturel m, l'équation $x^m = g$ admet une solution dans G. Un exemple de groupe complet est le groupe $\mathbf{UT}_n(K)$ sur un corps commutatif K de caractéristique nulle. En effet, posons par définition pour tous $a \in \mathbf{UT}_n(K)$, $\mu \in K$ en généralisant la formule (3):

$$a^\mu = \sum_{i=0}^{n-1} \binom{\mu}{i} (a-e)^i,$$

où

$$\binom{\mu}{i} = \frac{\mu(\mu-1)\ldots(\mu-i+1)}{i!}, \quad \binom{\mu}{0} = 1.$$

On vérifie immédiatement que

$$a^{\mu+\nu} = a^\mu a^\nu, \quad a^{\mu\nu} = (a^\mu)^\nu.$$

Il en découle en particulier que $a^{\frac{1}{m}}$ est une racine m-ième de a, i.e. que le groupe $\mathbf{UT}_n(K)$ est complet.

On dit qu'un groupe nilpotent complet sans torsion $\bar{G}$ est le *complété* (*nilpotent*) du groupe G s'il contient G et ne contient aucun sous-groupe propre complet contenant G.

17.3.1. Théorème. *Soit H sous-groupe d'un groupe nilpotent complet sans torsion G. L'ensemble $\sqrt{H}$ de tous les éléments de G qui figurent à une certaine puissance dans H (racine de H dans G) est un sous-groupe et, par conséquent, le complété de H dans G. Les hypercentres des sous-groupes H et $\sqrt{H}$ vérifient les relations suivantes:*

$$\zeta_i \sqrt{H} = \sqrt{\zeta_i H}, \quad \zeta_i H = H \cap \sqrt{\zeta_i H}.$$

Démonstration. a) Montrons d'abord que $\sqrt{H}$ est un sous-groupe, i.e. que $xy \in \sqrt{H}$ si $x \in \sqrt{H}$, $y \in \sqrt{H}$. Soient $A = (x, y)$, $B = A \cap H$, $A_i = \gamma_i A$. Il suffit de vérifier que tous les $|BA_i : BA_{i+1}| < \infty$ car on a alors $|A : B| < \infty$. La série

$$BA_1 \geqslant BA_2 \geqslant \ldots$$

est sous-normale à sections abéliennes, car on a en vertu des relations entre commutateurs (3) du n° 3.2

$$[BA_i, BA_i] \leqslant [B, B]^{A_i} [A_i, B]^{A_i} [A_i, A_i] \leqslant BA_{i+1}.$$

Soient x^m, $y^m \in B$; supposons démontré que la section BA_{i-1}/BA_i est finie et de période m^{i-1}. Montrons que la section BA_i/BA_{i+1} est de type fini et de période m^i. La première proposition est immédiate, puisque A est polycyclique (théorème 17.2.2). Ensuite, $[A_{i-1}, A, A] \equiv 1 \pmod{A_{i+1}}$, ce qui fait que la fonction $[u, v] \pmod{A_{i+1}}$, $u \in A_{i-1}$, $v \in A$, est homomorphe en ses deux arguments (toujours en vertu des relations entre commutateurs !). D'où

$$A_i^{m^i} = [A_{i-1}, A]^{m^i} \leqslant [A_{i-1}^{m^{i-1}}, A^m]\, A_{i+1}.$$

Puisque

$$A_{i-1}^{m^{i-1}} \leqslant (B \cap A_{i-1})\, A_i, \qquad A^m \leqslant BA_2,$$

on obtient en faisant intervenir, une fois de plus, les relations entre commutateurs

$$A_i^{m^i} \leqslant BA_{i+1},$$

ce qu'il fallait démontrer.

b) Pour démontrer les formules relatives aux hypercentres, introduisons la notation $H_i = \zeta_i H$ et passons de i à $i + 1$. On a tout d'abord $\zeta_{i+1} \sqrt{H} \leqslant \sqrt{H_{i+1}}$, car pour tout x de $\zeta_{i+1} \sqrt{H}$ on a $x^m \in H$ pour un m convenable et

$$[x^m, H] \leqslant H \cap \sqrt{H_i} = H_i,$$

d'où $x^m \in H_{i+1}$, $x \in \sqrt{H_{i+1}}$. Réciproquement, montrons que $\sqrt{H_{i+1}} \leqslant \zeta_{i+1}\sqrt{H}$, i.e. les sous-groupes $\sqrt{H}$, $\sqrt{H_{i+1}}$ commutent élément à élément modulo $\sqrt{H_i}$. Soient en effet $x \in \sqrt{H}$, $y \in \sqrt{H_{i+1}}$, i.e. $x^m \in H$, $y^n \in H_{i+1}$ pour des m, n convenables. Puisque $[H, H_{i+1}] \leqslant H_i \leqslant \sqrt{H_i}$, on a $x^m y^n \equiv y^n x^m \pmod{\sqrt{H_i}}$. Le groupe $\sqrt{H}/\sqrt{H_i}$ étant sans torsion (exercice 16.2.10), on a $xy \equiv yx \pmod{\sqrt{H_i}}$ (exercice 16.2.9), ce qu'il fallait démontrer.

Il reste à prouver que $H \cap \sqrt{H_{i+1}} = H_{i+1}$. Démontrons seulement l'inclusion non triviale $H \cap \sqrt{H_{i+1}} \leqslant H_{i+1}$. Soient $x \in H \cap \sqrt{H_{i+1}}$, $x^m \in H_{i+1}$. Alors x^m commute avec tout élément de H modulo H_i, ce qui est aussi vrai pour x (exercices 16.2.9 et 16.2.10). Il en ressort que $x \in H_{i+1}$. Le théorème est démontré.

17.3.2. Théorème (A. I. Maltsev). *Tout groupe nilpotent sans torsion G admet un complété nilpotent de même degré de nilpotence. Deux complétés nilpotents quelconques de G sont isomorphes. Il y a plus: pour tout automorphisme φ de G il existe entre ces deux complétés un isomorphisme qui prolonge φ.*

Démonstration. a) Unicité. Soient G_1, G_2 deux groupes isomorphes à G, φ un isomorphisme de G_1 sur G_2, $\sqrt{G_i}$ un complété nilpotent de G_i. Prenons le produit direct $P = \sqrt{G_1} \times \sqrt{G_2}$, isolons dans P un sous-groupe $D = \{xx^\varphi \mid x \in G_1\}$ et considérons sa racine $\sqrt{D}$ dans P. Vérifions que

$$P = \sqrt{D}\cdot\sqrt{G_i}, \quad \sqrt{D} \cap \sqrt{G_i} = 1 \quad \text{pour } i = 1, 2. \tag{8}$$

En effet, si $x \in \sqrt{D} \cap \sqrt{G_i}$, on a $x^m \in D \cap G_i$ pour un certain m. D'où $x = 1$; la deuxième formule (8) est démontrée. Il en ressort que la restriction de la projection $\pi: P \to \sqrt{G_1}$ au groupe $\sqrt{D}$ est un isomorphisme, d'où $\sqrt{D^\pi} = \sqrt{D^\pi}$. Ensuite, la restriction de π à $\sqrt{G_1}$ est aussi un isomorphisme, d'où $\sqrt{G^\pi} = \sqrt{G_1^\pi}$. Or, $D^\pi = G_1^\pi$, donc $\sqrt{D^\pi} = \sqrt{G_1^\pi}$. Revenant aux images réciproques par π, on obtient la première formule (8) pour $i = 2$. Par raison de symétrie elle reste vraie aussi pour $i = 1$.

Les formules (8) montrent que tout élément x_1 de $\sqrt{G_1}$ est projection d'un élément unique x de $\sqrt{D}$ sur le facteur $\sqrt{G_1}$. En associant à x_1 la projection de x sur $\sqrt{G_1}$, on obtient un isomorphisme de $\sqrt{G_1}$ sur $\sqrt{G_2}$ qui prolonge φ.

b) Existence. Si G est un groupe de type fini, il se plonge dans le groupe nilpotent complet $\mathrm{UT}_n(\mathbb{Q})$ pour un certain n (théorème 17.2.5). La racine $\sqrt{G}$ du sous-groupe G dans le groupe $\mathrm{UT}_n(\mathbb{Q})$ est un complété nilpotent de G. Etant donné un g de G et un entier naturel m, désignons par $\sqrt[m]{g}$ la solution de l'équation $x^m = g$ dans le groupe $\sqrt{G}$. Il est évident que

$$\sqrt[m]{g} = \sqrt[m']{g'} \Leftrightarrow g^{m'} = g'^{m} \tag{9}$$

et que, conformément à a), la table de multiplication dans $\sqrt{G}$ est complètement définie par celle dans G. Abandonnons maintenant l'hypothèse que G soit de type fini et considérons l'ensemble des symboles formels $\sqrt[m]{g}$, $g \in G$, $m = 1, 2, \ldots$ Introduisons dans cet ensemble la relation d'égalité définie par (9) et désignons par $\sqrt{G}$ l'ensemble des classes d'éléments égaux qu'on obtient dans ce cas. Convenons de multiplier $\sqrt[m]{g}$, $\sqrt[m']{g'}$ comme les éléments du complété nilpotent du groupe $\mathrm{gr}(g, g')$. Alors $\sqrt{G}$ devient un groupe qui contient le sous-groupe G. Si G est nilpotent de degré s, les complétés de ses sous-groupes de type fini sont nilpotents de degré $\leqslant s$ (théorème 17.3.1), aussi $\sqrt{G}$ vérifie-t-il l'identité $[x_1, \ldots, x_{s+1}] = 1$. Cela veut dire que $\sqrt{G}$ est un complété nilpotent de G de même degré de nilpotence que G. Le théorème est démontré.

Un groupe nilpotent qui contient des éléments périodiques ne se plonge pas toujours dans un groupe nilpotent complet, vu que la partie périodique du groupe nilpotent complet est toujours contenue dans le centre. En effet, on peut admettre par récurrence que tout élément périodique g de G appartient au deuxième hypercentre. Si $g^m = 1$, $m \neq 0$, on a $[g, x^m] = [g, x]^m = [g^m, x] = 1$ pour tout x de G. Puisque G est complet, x^m parcourt le groupe tout entier, si bien que g est un élément central.

§ 18. Généralisations de la nilpotence

La propriété de nilpotence admet un grand nombre de généralisations, dont nous ne considérons ici que trois: la nilpotence locale, la condition du normalisateur et la condition d'Engel.

18.1. Nilpotence locale. On dit qu'un groupe est *localement nilpotent* si tous ses sous-groupes de type fini sont nilpotents. Un tel groupe n'est pas nécessairement nilpotent lui-même, ainsi que le

montre l'exemple d'un produit direct de groupes nilpotents dont les degrés croissent à l'infini, ou l'exemple du groupe $\mathrm{UT}_\omega(K)$ de l'exercice 17.1.3. Plus généralement, si σ est une propriété du groupe héritée par les sous-groupes, on dit qu'un groupe G présente *localement* la propriété σ si tous ses sous-groupes de type fini ont la propriété σ (la définition pour σ quelconque sera formulée dans le chapitre suivant).

18.1.1. Exercice. Tout sous-groupe et tout groupe quotient d'un groupe localement nilpotent sont localement nilpotents eux-mêmes. Tout groupe localement nilpotent est localement polycyclique.

18.1.2. Théorème. 1° *Le produit de deux sous-groupes normaux localement polycycliques d'un groupe quelconque est un sous-groupe localement polycyclique.*

2° (B. I. Plotkine). *Le produit de deux sous-groupes normaux localement nilpotents d'un groupe quelconque est un sous-groupe localement nilpotent.*

Démonstration. 1° Soient K, L deux sous-groupes normaux localement polycycliques d'un groupe quelconque G. Il s'agit de montrer que tout sous-groupe de type fini dans KL est polycyclique. Choisissons un tel sous-groupe dans KL et mettons ses générateurs sous forme de produits ab, $a \in K$, $b \in L$. Soient A le sous-groupe engendré par les premiers facteurs et B, le sous-groupe engendré par les seconds. Par définition, A, B sont polycycliques. Il suffit visiblement de s'assurer que le groupe $H = \mathrm{gr}\,(A, B)$ qu'ils engendrent est polycyclique. Profitons du lemme 3.2.2 qui définit la structure de H (remarquons que dans notre cas les ensembles I, J, C sont finis). Compte tenu de ce lemme et de l'exercice 4.4.3, il suffit de vérifier que le groupe $A\,[A, B]$ est polycyclique.

Puisque K et L sont normaux dans G, on a $[K, L] \leqslant K \cap L$. Puisque A, $\mathrm{gr}\,(C)$ sont de type fini et sont contenus dans le groupe localement polycyclique K, le groupe $\mathrm{gr}\,(A, C)$ est polycyclique. Cela signifie que son sous-groupe $\mathrm{gr}\,(C^A)$ est polycyclique, lui aussi. D'autre part, il est contenu dans L, c'est pourquoi $\mathrm{gr}\,(\mathrm{gr}\,(C^A), B)$ est un sous-groupe de type fini de L, donc polycyclique. En vertu du lemme 3.2.2, il contient $[A, B]$. Aussi, $[A, B]$ est-il un groupe polycyclique. Puisque A et $[A, B]$ sont contenus tous deux dans K et sont de type fini, leur produit est un groupe polycyclique.

2° Même schéma de démonstration.

Il est bon maintenant, comme après le théorème de Fitting, de reprendre l'exercice 16.2.13.

Toutes les propriétés des groupes nilpotents énumérées dans le § 16 ne sont pas applicables aux groupes localement nilpotents:

par exemple, nous verrons dans l'exemple 18.2.2 que les sous-groupes des groupes localement nilpotents ne sont pas toujours sous-normaux. A quel point le théorème 16.2.2 s'applique-t-il alors aux groupes localement nilpotents? A ce titre, il convient de citer un

18.1.3. Théorème (D. H. McLain). *Tout sous-groupe maximal H d'un groupe localement nilpotent G est normal.*

Démonstration. Supposons au contraire que H ne soit pas normal dans G. Il existe alors un $x \in [G, G]$, $x \notin H$. Puisque H est maximal, on a $\mathrm{gr}\,(H, x) = G$. Soit

$$x = [y_1, z_1] \ldots [y_n, z_n], \quad y_i, z_i \in G.$$

Supposons que les y_i, z_i se laissent mettre sous la forme de mots en x et en $h_1, \ldots, h_m$ de H, et que

$$H^* = \mathrm{gr}\,(h_1, \ldots, h_m), \quad G^* = \mathrm{gr}\,(h_1, \ldots, h_m, x).$$

Par hypothèse, le groupe G^* est nilpotent. Il est évident que $x \in [G^*, G^*]$, $x \notin H^*$, aussi H^* est-il un sous-groupe propre de G^*. En vertu du théorème 16.2.2, le sous-groupe H^* figure parmi les termes d'une matriochka sous-normale de G^* qui, d'après le théorème 17.2.2, peut être subdivisée de façon à former une matriochka polycyclique

$$1 < \ldots < H^* < H_1 < \ldots < H_s < G^*. \tag{1}$$

Puisque la section G^*/H_s est commutative, on a $[G^*, G^*] \leqslant H_s$ donc $x \in H_s$. Or, on a alors $G^* \leqslant H_s$, ce qui contredit les inclusions strictes (1). Le théorème est démontré.

18.1.4. Exercice. Dans tout groupe localement nilpotent G, les éléments périodiques constituent un sous-groupe (appelé *partie périodique* de G).

Indication: voir le théorème 16.2.7.

18.1.5. Exercice. Tout groupe périodique, localement nilpotent se décompose en produit direct de ses sous-groupes de Sylow.

Indication. Compte tenu de l'exercice 16.1.6 et du théorème 17.1.4, montrer que pour tout nombre premier p il existe un seul p-sous-groupe de Sylow.

18.2. Condition du normalisateur. H. Heineken et I. J. Mohamed ont montré (J. Algebra, 1968, **10**, p. 368-376) que la réciproque du théorème 16.2.2 n'est pas vraie en général, i.e. qu'il existe des groupes non nilpotents dont tous les sous-groupes sont sous-normaux. Remarquons cependant que pour tout entier naturel n il existe des entiers naturels $r(n)$, $s(n)$ tels que tout groupe dont tout sous-groupe à $r(n)$ générateurs intervient dans une série sous-normale de

longueur $\leqslant n$ soit un groupe nilpotent de degré $\leqslant s(n)$ (cf. J. E. Roseblade in: *J. Algebra*, 1965, 2, n° 4, p. 402-412).

Moins restrictive que la condition de sous-normalité de tous les sous-groupes, la *condition du normalisateur* veut que tout sous-groupe propre soit distinct de son normalisateur.

18.2.1. Théorème (B. I. Plotkine). *Tout groupe G vérifiant la condition du normalisateur est localement nilpotent.*

Démonstration. En vertu du lemme de Zorn, tout élément de G appartient à un sous-groupe maximal, localement nilpotent H. Il suffit de montrer que H est normal dans G (auquel cas G est recouvert de sous-groupes normaux, localement nilpotents, ce qui signifie, en vertu du théorème 18.1.2, qu'il est localement nilpotent lui-même). Introduisons la notation $N = N_G(H)$. Si $N^g = N$, alors H^g, H sont normaux dans N. En vertu du théorème 18.1.2, leur produit H^gH est localement nilpotent. Puisque H est maximal, on a $H^gH = H$, d'où $H^g = H$, $g \in N$. Ainsi donc, N se confond avec son normalisateur. Conformément à la condition du normalisateur, on a $N = G$, ce qu'il fallait démontrer.

La réciproque de ce théorème est fausse, ce que nous allons voir à l'aide d'un exemple dont la portée ne s'arrête d'ailleurs pas là.

18.2.2. Exemple (M. I. Kargapolov). Définissons pour tout α transfini un groupe G_α tel que

$$G_0 = C_p, \quad G_\alpha = \begin{cases} C_p \wr G_{\alpha-1} & \text{pour } \alpha \text{ non limite,} \\ \bigcup\limits_{\beta<\alpha} G_\beta & \text{pour } \alpha \text{ limite.} \end{cases}$$

Par construction, chaque G_α est un p-groupe dont tous les sous-groupes de type fini sont finis et $|G_\alpha| \geqslant |\alpha|$. En particulier, tous les G_α sont localement nilpotents.

Soit γ le premier ordinal transfini non dénombrable. Il est clair que pour $\alpha < \gamma$ tous les G_α sont dénombrables, tandis que G_γ est non dénombrable. Montrons que G_γ ne vérifie pas la condition du normalisateur. En effet, s'il la vérifiait, il y aurait dans G_γ une suite de sous-groupes H_λ indiciés par des ordinaux transfinis $\lambda \leqslant \nu$ tels que

a) $H_0 = 1$, $H_\mu \lhd H_{\mu+1}$, $H_\lambda = \bigcup\limits_{\mu<\lambda} H_\mu$ pour λ limite, $H_\nu = G_\gamma$,

b) toutes les sections $H_{\mu+1}/H_\mu$ seraient commutatives.

(On pourrait construire une telle suite par exemple en prenant comme H_λ le groupe défini par la première et la troisième formules de a), et comme $H_{\mu+1}$, le groupe engendré par H_μ et un élément quelconque de $N(H_\mu)$ extérieur à H_μ.) Nous allons montrer qu'en

réalité le groupe G_γ ne contient aucun sous-groupe vérifiant les conditions a) et b).

Supposons au contraire qu'il existe des sous-groupes pareils H_λ. Faisant intervenir au besoin des termes convenables dans leur suite, on peut admettre que toutes les sections $H_{\mu+1}/H_\mu$ sont cycliques. Alors tous les H_n indiciés par des entiers naturels n sont dénombrables, de même que leur réunion H_ω. Numérotons les éléments de H_ω: $h_1, h_2, \ldots$ Il est évident que $h_m \in G_{\beta_m}$ pour un $\beta_m < \gamma$. La réunion de tous les G_{β_m} est un G_β, tel que $\beta < \gamma$, car G_β est dénombrable et G_γ ne l'est pas. Nous aboutirons à une contradiction en montrant que G_β contient tous les H_λ pour $\omega < \lambda \leqslant \nu$. A cet effet, raisonnons par récurrence sur λ. Pour les λ limites, la proposition est évidente: soit donc λ un ordinal non limite. Supposons démontré que $H_{\lambda-1} \leqslant G_\beta$, mais qu'il existe un $h \in H_\lambda$, $h \notin G_\beta$. Soit un α tel que $h \in G_\alpha$, $h \notin G_{\alpha-1}$. De toute évidence, $\beta \leqslant \alpha - 1$, donc $H_{\lambda-1} \leqslant G_{\alpha-1}$. Par définition d'un entrelacement

$$h = bf, \quad b \in G_{\alpha-1}, \quad f \in \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p),$$

et ceci pour $f \neq 1$. Pour tout $x \in H_{\lambda-1}$ on a

$$[x^b, f] = x^{-b}x^{bf} \in G_{\alpha-1} \cap \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p) = 1,$$

i.e. $H^b_{\lambda-1}$ centralise f. L'élément $f' = bfb^{-1} \neq 1$ admet donc un centralisateur infini dans $G_{\alpha-1}$. D'autre part, ce centralisateur, opérant sur $G_{\alpha-1}$ par translations à droite, doit renvoyer supp (f') dans lui-même. Il est donc isomorphe à un groupe de permutations d'un ensemble fini supp (f') et, pour cette raison, ne peut pas être infini.

18.2.3. Exercice. Le groupe G_γ admet un centre trivial.

Les groupes vérifiant la condition du normalisateur sont à tel point proches des groupes à matriochkas centrales (infinies, en général) qu'on a longtemps ignoré s'il existe des groupes vérifiant la condition du normalisateur et dépourvus de centre. La réponse positive à cette question a été apportée par H. Heineken et I. J. Mohamed (voir la référence citée au commencement de ce n°).

Cependant, on ignore toujours ([13], question 2.80) si un groupe arbitraire vérifiant la condition du normalisateur admet un sous-groupe normal abélien non trivial.

18.3. Condition d'Engel. La source de cette généralisation est la relation entre commutateurs

$$[x_0, x_1, \ldots, x_n] = 1 \tag{2}$$

qui, comme nous le savons, définit des groupes nilpotents de degré $\leqslant n$. Le désir de réduire autant que possible le nombre des variables

nous conduit à la relation

$$[x, \underbrace{y, \ldots, y}_{n}] = 1 \tag{3}$$

(il va sans dire que l'absence des crochets intérieurs signifie leur « bonne disposition »: $[[[x, y], y], \ldots, y]$). Un groupe qui vérifie la relation (3) s'appelle *groupe incomplètement engélien* de degré $\leqslant n$, du nom de F. Engel qui, avec Sophus Lie, a posé les bases de la théorie des groupes de Lie et des algèbres de Lie, mentionnée au commencement du chapitre. Il est évident que la variété des groupes incomplètement engéliens de degré $\leqslant n$ contient la variété de tous les groupes nilpotents de degré $\leqslant n$. Cependant, ces variétés ne se confondent pas, comme le montre un

18.3.1. Exemple (K. Weston). Soit M l'ensemble des entiers naturels qui sont « square-free », i.e. qui se décomposent en produit de nombres premiers distincts. A chaque $m \in M$, associons un groupe cyclique du second ordre à générateur a_m et désignons par A le produit direct de tous les (a_m). A chaque p premier sera associé un automorphisme φ_p du groupe A, défini sur les générateurs par les formules suivantes:

$$a_m^{\varphi_p} = \begin{cases} a_m a_{m/p} & \text{si } p \mid m, \\ a_m & \text{sinon.} \end{cases}$$

Il est évident que $\varphi_p^2 = 1$ et $\varphi_p \varphi_q = \varphi_q \varphi_p$, si bien que le groupe Φ engendré par tous les φ_p est commutatif de période 2. Soit G l'extension de A par Φ (voir n° 6.1). Par définition, si q ne divise pas m, on a

$$a_m = [a_{mq}, \varphi_q].$$

D'où $[G, G] = A$, $[G, A] = A$, ce qui signifie que le groupe G n'est pas nilpotent. D'autre part, il vérifie la relation $[x, y, y, y] = 1$. En effet, si $a, a' \in A$, $\varphi, \varphi' \in \Phi$, on a successivement $[a, a'\varphi] = [a, \varphi]$ en vertu de l'identité $[x, yz] = [x, z][x, y]^z$ et de la commutativité du groupe A; $[a, \varphi, \varphi] = 1$ en vertu de l'identité $[x, y, z] = [y, x][z, x][x, yz]$ et de la relation $[a, \varphi]^2 = 1$; enfin, $[a\varphi, a'\varphi', a'\varphi', a'\varphi'] = [a\varphi, a'\varphi', \varphi', \varphi'] = 1$ en vertu de ce qui précède. Remarquons en outre le fait évident que le groupe de Weston est de période 4.

Un groupe est dit *engélien* si pour ses deux éléments quelconques x, y la relation (3) a lieu pour un certain n qui dépend en général de ces éléments. Il est évident que la classe des groupes engéliens contient la classe de tous les groupes localement nilpotents. Ces deux classes ne se confondent pourtant pas, comme le montre un

18.3.2. Exemple (E. S. Golod). Pour tout $d \geqslant 2$, il existe un groupe G non nilpotent à d générateurs dont tout sous-groupe à $d - 1$ générateurs est nilpotent. Un tel groupe se laisse construire à l'aide d'un exemple analogue pour les algèbres, plus exactement à l'aide d'une algèbre A non nilpotente (de dimension infinie) à d générateurs dont toute sous-algèbre à $d - 1$ générateurs est nilpotente. Cette construction, décrite en détail dans le § 26 de l'Appendice, met A sous la forme F'/I, où F' est la sous-algèbre des « polynômes sans terme constant » de l'algèbre associative libre F à générateurs $x_1, \ldots, x_d$ sur un corps commutatif k quelconque, et I un idéal homogène dans F'. Soient p un nombre premier et $k = \mathrm{GF}(p)$. Prenons dans F/I l'ensemble

$$1 + A = \{1 + a \mid a \in A\}.$$

Il est évident que $(1 + a)(1 + b) = 1 + a + b + ab$, $(1 + a)^{-1} = 1 - a + a^2 - \ldots + (-1)^{n-1}a^{n-1}$ si $a^n = 0$, donc $1 + A$ est un groupe. Ensuite, pour tout $a \in A$ il existe un m tel que $a^{p^m} = 0$, d'où

$$(1+a)^{p^m} = \sum_{i=0}^{p^m} \binom{p^m}{i} a^i = 1,$$

puisque tous les coefficients binomiaux, sauf le premier et le dernier, se divisent par p. Donc $1 + A$ est un p-groupe. Soit G son sous-groupe engendré par les éléments $1 + \bar{x}_1, \ldots, 1 + \bar{x}_d$, où $\bar{x}_i = x_i + I$. Il est clair que le sous-groupe engendré par les éléments $1 + a_1, \ldots, 1 + a_{d-1}$, $a_i \in A$, est contenu dans $1 + A^*$, où A^* est la sous-algèbre engendrée par les éléments $a_1, \ldots, a_{d-1}$. Par hypothèse, l'algèbre A^* est nilpotente; il en est donc de même pour le groupe $1 + A^*$ (exercice 16.1.4). Ainsi donc, tous les sous-groupes de G, à $d - 1$ générateurs sont nilpotents, mais le groupe G lui-même n'est pas nilpotent. En effet, s'il n'en était pas ainsi, G serait fini en vertu des résultats de l'exercice 16.1.6. Or, l'anneau de groupe $k[G]$ et son image homomorphe canonique $F/I = k \oplus A$ seraient finis tous les deux, alors que l'algèbre A est infinie comme annoncé.

On ignore actuellement si tout groupe est localement nilpotent si pour ses deux éléments quelconques x, y la relation (3) est vérifiée avec un n qui ne dépend que de y. On ignore aussi si dans tout groupe le produit des sous-groupes normaux engéliens est encore un sous-groupe engélien.

CHAPITRE 7

GROUPES RÉSOLUBLES

§ 19. Propriétés générales et exemples

19.1. Définitions. Comme nous l'avons dit au commencement du chapitre précédent, les groupes résolubles sont ceux qui se déduisent des groupes abéliens par extensions successives. Il existe d'autres définitions équivalentes de la résolubilité.

19.1.1. Théorème. *Pour un groupe G quelconque, les propositions suivantes sont équivalentes:*

a) *le groupe G admet une matriochka sous-normale à sections abéliennes,*

b) *le groupe G admet une matriochka normale à sections abéliennes,*

c) *la série dérivée $G \geqslant G' \geqslant \ldots \geqslant G^{(n)} \geqslant \ldots$ du groupe G devient stationnaire sur 1 au bout d'un nombre fini de pas, i.e. cette série est une matriochka (finie),*

d) *le groupe G vérifie une des identités*

$$\delta_n (x_1, \ldots, x_{2^n}) = 1, \quad n = 0, 1, 2, \ldots,$$

où $\delta_0 (x) = x$, $\delta_{n+1} (x_1, \ldots, x_{2^{n+1}}) = [\delta_n (x_1, \ldots, x_{2^n}), \delta_n (x_{2^n+1}, \ldots, x_{2^{n+1}})]$.

Démonstration. c) $\Rightarrow$ b) $\Rightarrow$ a): c'est évident.

a) $\Rightarrow$ c). Supposons que le groupe G admet une matriochka sous-normale à sections abéliennes:

$$1 = H_0 < H_1 < \ldots < H_s = G.$$

Puisque le groupe quotient G/H_{s-1} est abélien, on a $G' \leqslant H_{s-1}$. Supposons démontrée l'inclusion $G^{(k)} \leqslant H_{s-k}$, $1 \leqslant k < s$. Du fait que la section H_{s-k}/H_{s-k-1} est commutative, le commutant $(G^{(k)})' = G^{(k+1)}$ est contenu dans H_{s-k-1}. D'où $G^{(s)} = 1$. Nous avons donc montré que les trois premières propositions sont équivalentes.

c) $\Rightarrow$ d). Supposons que le s-ième commutant $G^{(s)}$ du groupe G est égal à l'unité. Puisque le $(s-1)$-ième commutant du groupe

$G/G^{(s-1)}$ est égal à l'unité, on peut admettre par récurrence que $\delta_{s-1}(g_1, \ldots, g_{2^{s-1}}) \in G^{(s)}$, où $\delta_{s-1}(g_1, \ldots, g_{2^{s-}})$ est la valeur prise par le mot δ_{s-1} sur les éléments g_i. De ce fait et en vertu de la commutativité du groupe $G^{(s)}$, on a $\delta_s(g_1, \ldots, g_{2^s}) = 1$ pour tout $g_i \in G$.

d) $\Rightarrow$ c). Réciproquement, supposons que $\delta_s = 1$ sur G. Il est évident que le sous-groupe H engendré par les valeurs du mot δ_{s-1} est normal et commutatif. Sur le groupe quotient G/H on a $\delta_{s-1} = 1$, d'où $G^{(s-1)} \leqslant H$ et par conséquent $G^{(s)} = 1$. Le théorème est démontré.

On dit que le groupe G est *résoluble* si une des propositions a), b), c), d) a lieu sur G. Les matriochkas indiquées dans les propositions a), b) sont appelées *résolubles*, elles aussi. Etant donné un groupe résoluble G, on appelle *degré de résolubilité* de G le plus petit nombre positif n pour lequel $G^{(n)} = 1$.

De la démonstration du théorème 19.1.1 on voit que l'identité $\delta_n = 1$ a lieu sur les groupes résolubles de degré $\leqslant n$, et sur ces groupes seulement. Par conséquent, la classe des groupes résolubles de degré $\leqslant n$ est une variété. Il en découle immédiatement que la classe des groupes résolubles est fermée par rapport à la prise de sous-groupes, d'images homomorphes et de produits directs finis, ainsi que par rapport à la prise de produits cartésiens, à condition que les degrés de résolubilité des facteurs soient bornés. Un produit direct (cartésien) de groupes résolubles quelconques peut être un groupe non résoluble.

19.1.2. Exercice. Les groupes matriciels trigonaux $\mathbf{T}_n(K)$ sont résolubles. Leur produit direct pour $n = 1, 2, \ldots$ n'est pas un groupe résoluble.

19.1.3. Exercice. L'extension d'un groupe résoluble par un groupe résoluble est encore résoluble.

19.1.4. Exercice. Le produit de deux sous-groupes normaux résolubles d'un groupe est un sous-groupe résoluble.

19.1.5. Exercice. Etant donné un groupe fini quelconque G, il existe un et un seul sous-groupe normal résoluble N tel que le groupe quotient G/N ne contienne aucun sous-groupe normal abélien non trivial.

19.1.6. Exercice. Tout groupe résoluble fini admet une matriochka sous-normale à sections cycliques d'ordres premiers.

19.1.7. Exercice. Tout sous-groupe normal minimal d'un groupe résoluble fini est un groupe abélien élémentaire, i.e. se décompose en produit direct de groupes cycliques de même ordre premier.

19.1.8. Exercice. Tout groupe résoluble périodique de type fini est fini (cf. l'exercice 16.1.6).

19.1.9. Exercice. Soient p un nombre premier et T_p un groupe de matrices de la forme

$$\begin{pmatrix} 1 & * & * & * \\ & * & * & * \\ & & * & * \\ & & & 1 \end{pmatrix}$$

sur l'anneau $\mathbb{Q}_p$ des fractions p-aires à éléments diagonaux strictement positifs. On demande de montrer que

1° le centre $Z(T_p)$ du groupe T_p est formé de matrices qui ont une étoile unique à l'angle supérieur de droite, donc isomorphe au groupe additif $\mathbb{Q}_p$,

2° le groupe T_p est engendré par les matrices diagonales

$$d_2 = \operatorname{diag}(1, p, 1, 1), \quad d_3 = \operatorname{diag}(1, 1, p, 1)$$

et les transvections $t_{ij} = e + e_{ij}$, $i < j$.

H. Abels a montré (*London Math. Soc. Lecture Note Ser.*, 1979, 36, p. 205-211) que T_p admet en ces générateurs un code génétique fini

$$[d_2, d_3] = 1, \quad [t_{ij}, t_{kl}] = t_{il}^{\delta(j,k)}, \quad t_{i,i+1}^{p\,\delta(i,j)} d_j = d_j t_{i,i+1}^{p\,\delta(i+1,j)},$$

où $\delta(i, j)$ désigne l'unité pour $i = j$ et zéro dans le cas contraire. Ainsi donc, T_p est un exemple de groupes résolubles de présentation finie dont le centre n'est pas de type fini et qui admettent des suites strictement croissantes infinies $N_1 < N_2 < \ldots$ de sous-groupes normaux (et même centraux).

Un autre exemple important, qui met en lumière non pas la complexité structurelle mais la complexité algorithmique des groupes résolubles de présentation finie, a été indiqué assez récemment par O. G. Kharlampovitch (in *Izv. AN SSSR, ser. matem.*, 1981, 45, n° 4, p. 852-873) : il s'agit d'un groupe résoluble de degré 3 à code génétique fini :

$$G = \operatorname{gr}(x_1, \ldots, x_n \mid\mid v_1 = 1, \ldots, v_m = 1)$$

sur lequel le problème d'égalité n'a pas de solution. Cela veut dire qu'il n'existe pour G aucun algorithme qui, étant donnés deux mots quelconques en alphabet $x_1, \ldots, x_n$, permette de conclure à leur égalité ou inégalité en tant qu'éléments de G.

19.2. Groupes polycycliques et groupes hyperrésolubles. Un exemple évident de groupes résolubles est fourni par les groupes polycycliques. Une sous-classe importante des groupes polycycliques est constituée par les *groupes hyperrésolubles* : ce sont les groupes qui admettent une matriochka normale (et non simplement sous-normale

comme précédemment) à sections cycliques. Un exemple déjà familier de groupes hyperrésolubles est représenté par les groupes nilpotents de type fini.

19.2.1. Exercice. Tout sous-groupe et tout groupe quotient d'un groupe hyperrésoluble sont hyperrésolubles.

19.2.2. Théorème. *Le commutant d'un groupe hyperrésoluble est nilpotent.*

Démonstration. Soit dans le groupe G une matriochka normale polycyclique $1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G$, et soit G' le commutant de G. En vertu du théorème 4.4.2, la série

$$1 = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_n = G', \quad \text{où} \quad H_i = G_i \cap G',$$

est une matriochka normale polycyclique dans G'. Montrons qu'en réalité elle est centrale dans G', i.e. que $[G', H_{i+1}] \leqslant H_i$ pour tout $i = 0, 1, 2, \ldots, n-1$. Il est évident que les conjugaisons de G par les éléments de G induisent des automorphismes dans les sections H_{i+1}/H_i. Puisque les automorphismes d'un groupe cyclique forment un groupe abélien (voir les exemples 5.1.1), le commutant G' doit induire une transformation identique dans toutes les sections H_{i+1}/H_i. Or, cela confirme les inclusions cherchées. Le théorème est démontré.

Notons encore une propriété des groupes hyperrésolubles finis.

Soit G un groupe fini d'ordre $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, où p_i sont des nombres premiers, $p_1 > \ldots > p_k$. Une matriochka normale

$$1 = H_0 < H_1 < \ldots < H_k = G$$

s'appelle *matriochka de Sylow* dans G si sa section H_{i+1}/H_i, $i = 0, 1, \ldots, k-1$, est un p_{i+1}-sous-groupe de Sylow dans le groupe G/H_i. (On omet quelquefois, dans cette définition, d'exiger que la suite $p_1 > \ldots > p_k$ soit ordonnée.)

19.2.3. Théorème. *Tout groupe hyperrésoluble fini admet une matriochka de Sylow.*

Démonstration. Soit p le plus grand diviseur premier de l'ordre du groupe hyperrésoluble G, et soit H un sous-groupe normal d'ordre premier q dans G. Le groupe quotient G/H est hyperrésoluble et $|G/H| < |G|$. Par hypothèse de récurrence, nous pouvons admettre que le p-sous-groupe de Sylow P/H est normal dans le groupe quotient G/H. Pour $p = q$, le sous-groupe P est un p-sous-groupe de Sylow dans G et $P \trianglelefteq G$. Si $p \neq q$, il existe dans G/H un sous-groupe normal H_1/H d'ordre p. Le théorème de Sylow permet de voir sans peine que le p-sous-groupe de Sylow H_2 de H_1 est unique et, en vertu de la relation $H_1 \trianglelefteq G$, normal dans G. Appli-

quant de nouveau le raisonnement par récurrence à G/H_2, on s'assure que le p-sous-groupe de Sylow de G est normal. La démonstration est en principe achevée.

§ 20. Groupes résolubles finis

Remarquons tout d'abord que les groupes résolubles finis ne sont autres que les groupes polycycliques finis.

Dans le premier n° de ce paragraphe nous exposons la théorie des sous-groupes de Hall et de Carter dans un groupe résoluble fini, théorie qui rappelle celle des p-sous-groupes de Sylow dans un groupe fini quelconque. Dans le troisième n° nous indiquons un critère d'hyperrésolubilité d'un groupe fini. Le deuxième n° a un caractère préparatoire, mais les théorèmes de Maschke et de Schur sur les groupes finis arbitraires revêtent une importance capitale intrinsèque.

20.1. Sous-groupes de Hall et de Carter. En vertu du théorème de Sylow 11.1.1, il existe toujours dans un groupe fini quelconque d'ordre $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ (p_i nombres premiers distincts) un sous-groupe d'ordre $p_i^{\alpha_i}$, et deux sous-groupes quelconques de ce type sont conjugués entre eux. Ph. Hall a généralisé le théorème de Sylow pour les groupes résolubles finis en démontrant que pour tout groupe résoluble fini G d'ordre n et tout nombre k tel que $k \mid n$, $\left(k, \frac{n}{k}\right) = 1$ il existe dans G des sous-groupes conjugués d'ordre k. De tels diviseurs de n sont appelés *diviseurs de Hall*, et tout sous-groupe dont l'ordre est égal à un diviseur de Hall de l'ordre du groupe donné s'appelle *sous-groupe de Hall*. Remarquons sans démonstration le résultat suivant: si pour tout diviseur de Hall de l'ordre d'un groupe fini G il existe dans G un sous-groupe de Hall, alors G est un groupe résoluble. Ce résultat est dû à Ph. Hall (*J. London Math. Soc.*, 1937, **12**, p. 198-200) et à S. A. Tchounikhine (*Izv. NIIMM Tomskogo oun-ta*, 1938, **2**, p. 220-223).

20.1.1. Théorème (Ph. Hall). *Soient G un groupe résoluble fini d'ordre n, et k un diviseur de Hall de n. Alors*

1° *il existe dans G au moins un sous-groupe d'ordre k,*

2° *deux sous-groupes quelconques d'ordre k sont conjugués dans G,*

3° *tout sous-groupe d'ordre $k' \mid k$ est contenu dans un sous-groupe d'ordre k.*

Démonstration. Raisonnons par récurrence sur n. Supposons que toutes les propositions énumérées ont lieu pour un groupe résoluble fini quelconque d'ordre inférieur à n. Désignons par A un

sous-groupe normal minimal dans G. Conformément à l'exercice 19.1.7, le sous-groupe A se décompose en produit direct de sous-groupes cycliques d'ordre premier p, $|A| = p^m$.

Si $p \mid k$, il existe dans le groupe quotient G/A, par hypothèse de récurrence, un sous-groupe B/A d'ordre k/p^m. L'ordre de B est alors égal à k. En outre, n'importe quels sous-groupes B_1, B_2 d'ordre k contiennent visiblement A. Par récurrence, les sous-groupes B_1/A et B_2/A sont conjugués dans G/A. Il en découle que les sous-groupes B_1, B_2 sont conjugués dans G.

Supposons maintenant que p ne divise pas k. Désignons par D le plus grand sous-groupe normal de G dont l'ordre est premier avec k, et par H/D un sous-groupe normal minimal dans G/D. L'ordre de H/D est de la forme q^s, où $q^s \mid k$.

Si le normalisateur $N(Q)$ d'un q-sous-groupe de Sylow Q de H se confond avec G, on a $Q \trianglelefteq G$; les propositions 1°, 2° sont démontrées de la même façon que précédemment, dans l'hypothèse que $p \mid k$.

Soit $N(Q) \neq G$. De l'égalité $G = N(Q)\,H = N(Q)\,D$ (voir le lemme de Frattini 17.1.8) il ressort que l'ordre de $N(Q)$ est divisible par k. Il existe donc, par hypothèse de récurrence, des sous-groupes d'ordre k dans $N(Q)$ et, par conséquent, dans le groupe G.

Prenons deux sous-groupes B_1, B_2 d'ordre k. Les intersections $B_1 \cap H$, $B_2 \cap H$ sont des q-sous-groupes de Sylow dans H ; puisqu'ils sont conjugués, on peut admettre que $B_1 \cap H = B_2 \cap H = Q$. Il est évident que Q est un sous-groupe normal dans le sous-groupe (B_1, B_2). Les sous-groupes B_1/Q, B_2/Q sont par récurrence conjugués dans $(B_1, B_2)/Q$, d'où la conjugaison des sous-groupes B_1, B_2.

Les propositions 1°, 2° sont donc démontrées. Passons à la proposition 3°.

Soit B' un sous-groupe d'ordre k'. Si $p \mid k$, l'ordre du sous-groupe AB' divise évidemment k. Par hypothèse de récurrence, le sous-groupe AB'/A est contenu dans un sous-groupe d'ordre k/p^m. Alors AB' est contenu dans un sous-groupe d'ordre k.

Supposons maintenant que p ne divise pas k. Par hypothèse de récurrence, le sous-groupe AB'/A est contenu dans un sous-groupe C/A d'ordre k. Par le même raisonnement, $C = G$. En vertu de la proposition 1° démontrée ci-dessus, il existe dans G un sous-groupe B d'ordre k. Il est évident que le produit AB se confond avec G, d'où $AB'B = G$. Des formules

$$|G| = \frac{|AB'|\cdot|B|}{|AB' \cap B|}, \quad |G| = p^m k, \quad |AB'| = p^m k', \quad |B| = k$$

il ressort que l'ordre de $D = AB' \cap B$ est égal à k'. En vertu de la proposition 2° démontrée ci-dessus, les sous-groupes B' et D sont conjugués dans AB' : $B' = D^g$. Il en découle que B' est contenu dans le sous-groupe B^g d'ordre k. Le théorème est démontré.

20.1.2. Exercice. L'indice d'un sous-groupe maximal quelconque d'un groupe résoluble fini est une puissance d'un nombre premier. Pour tout diviseur premier p de l'ordre du groupe G, il existe un sous-groupe maximal dans G dont l'indice est une puissance de p.

20.1.3. Exercice. Soit A un sous-groupe de Hall dans un groupe résoluble fini G, et soit H un sous-groupe contenant son normalisateur $N_G(A)$. Alors $N_G(H) = H$.

Ph. Hall a introduit la notion de base de Sylow et généralisé son théorème en ces termes, ce qui a provoqué une série d'autres généralisations.

L'ensemble $G_{p_1}, G_{p_2}, \ldots$ des p_i-sous-groupes de Sylow d'un groupe G s'appelle *base (complète) de Sylow* si

1° $G = \mathrm{gr}\,(G_{p_1}, G_{p_2}, \ldots)$,

2° $G_{p_i}G_{p_j} = G_{p_j}G_{p_i}$ pour tous i, j.

Parfois, la condition 2° de cette définition est remplacée par

2'° L'ensemble des diviseurs premiers des ordres des éléments du sous-groupe $\mathrm{gr}\,(G_{p_{i_1}}, \ldots, G_{p_{i_s}})$ se confond avec $\{p_{i_1}, \ldots, p_{i_s}\}$ pour tous les $i_1, \ldots, i_s$.

Ces définitions s'avèrent équivalentes en général.

On dit que deux bases de Sylow $\{G_{p_i}\}$, $\{G'_{p_i}\}$ sont *conjuguées* s'il existe un élément g tel que $G'_{p_i} = G^g_{p_i}$ pour tout i.

La généralisation effectuée par Hall (*Proc. London Math. Soc.*, 1937, 43, p. 316-323) consiste en ce qui suit. Tout groupe résoluble fini G admet des bases de Sylow qui sont conjuguées deux à deux dans G. Toute base de Sylow d'un sous-groupe de G se laisse prolonger en une base de Sylow dans G.

La notion de base de Sylow reste valable pour des groupes périodiques quelconques, aussi est-il naturel d'essayer d'étendre le théorème sur l'existence des bases de Sylow aux groupes résolubles périodiques. Bien que de pareilles extensions aient été obtenues pour certaines classes de groupes infinis, tout groupe résoluble périodique n'admet pas nécessairement des bases de Sylow (M. I. Kargapolov in: *DAN SSSR*, 1959, 127, n° 6, p. 1164-1166; *Alguebra i loguika*, 1963, 2, n° 5, p. 19-28).

On dit que le sous-groupe H d'un groupe G est un *sous-groupe de Carter* si H est nilpotent et se confond avec son normalisateur dans G.

20.1.4. Théorème (Carter). *Tout groupe résoluble fini G admet au moins un sous-groupe de Carter; tous les sous-groupes de Carter de G sont conjugués deux à deux.*

Démonstration. Raisonnons par récurrence sur l'ordre de G.

Soient A un sous-groupe normal minimal dans G et $|A| = p^m$. Par hypothèse de récurrence, le groupe quotient G/A admet un sous-groupe de Carter, par exemple K'/A. Soit Q un p'-sous-groupe de Hall du groupe K', i.e. p ne divise pas $|Q|$ et $|K'| = |Q|p'$. Montrons que $K = N_{K'}(Q)$ est un sous-groupe de Carter dans G.

En effet, on a d'après le lemme de Frattini généralisé 17.1.9, $K' = N_{K'}(Q) \cdot QA = KA$. Le sous-groupe K se décompose en produit direct des sous-groupes nilpotents Q et $K \cap P$, où P est un p-sous-groupe de Sylow de K'. Donc, le sous-groupe K est nilpotent. Soit ensuite $K^g = K$. Puisque $A \trianglelefteq G$ et que $K' = KA$, on a $K'^g = K'$ et donc $g \in K'$. Le normalisateur d'un sous-groupe de Hall se confond avec son propre normalisateur (voir l'exercice 20.1.3), aussi g appartient-il à K, ce qu'il fallait démontrer.

Soient maintenant K_1, K_2 deux sous-groupes de Carter dans le groupe G. Il s'agit de montrer qu'ils sont conjugués dans G.

Montrons d'abord que K_iA/A, $i = 1, 2$, est un sous-groupe de Carter du groupe G/A. La nilpotence du sous-groupe K_iA/A est évidente. Si $(K_iA)^g = K_iA$, $g \notin K_iA$, on aurait $|K_iA| < |G|$ et il existerait donc, par hypothèse de récurrence appliquée aux sous-groupes de Carter dans K_iA, un élément $a \in K_iA$ tel que $K_i^g = K_i^a$ ou $K_i^{ga^{-1}} = K_i$. Or, le sous-groupe K_i se confond avec son normalisateur, si bien que $ga^{-1} \in K_i$, ce qui contredit l'hypothèse selon laquelle $g \notin K_iA$.

On voit sans peine qu'un p'-sous-groupe de Hall Q_i de K_i est un p'-sous-groupe de Hall dans K_iA. En outre, le normalisateur $N(Q_i)$ de Q_i dans K_iA est nilpotent et contient K_i. Par conséquent, K_i se confond avec $N(Q_i)$. Par hypothèse de récurrence, les sous-groupes de Carter K_1A/A, K_2A/A sont conjugués entre eux. On peut donc admettre que $K_1A = K_2A$. Nous avons remarqué que le sous-groupe K_i se confond avec le normalisateur $N(Q_i)$ dans K_1A. Or, les p'-sous-groupes de Hall Q_1, Q_2 de K_1, K_2, étant des p'-sous-groupes de Hall dans K_1A, sont conjugués entre eux. Il en est donc de même pour leurs normalisateurs, soit pour K_1 et K_2. Le théorème est démontré.

20.2. Sur la réductibilité complète des représentations. Nous ferons une petite digression en théorie des représentations matricielles. Le but poursuivi dans ce n° consiste à exposer le théorème classique de Maschke sur la réductibilité complète des représentations des groupes finis. Nous aurons besoin de ces représentations dans le n° suivant. D'autres renseignements sur la réductibilité complète seront également donnés en passant.

Soient V un espace vectoriel sur un corps commutatif K_1 et G un groupe de transformations linéaires de V. S'il existe dans V un sous-espace propre permis par rapport à G, on dit que G est un *groupe*

réductible. Sinon, on dit que G est *irréductible* ou qu'il *opère irréductiblement* sur V. Le groupe G est dit *complètement réductible* si pour tout sous-espace permis $U \leqslant V$ il existe un supplémentaire permis, i.e. un sous-espace permis W tel que $V = U \oplus W$.

Tout homomorphisme φ d'un groupe abstrait G dans le groupe des transformations linéaires d'un espace vectoriel à n dimensions sur un corps commutatif K s'appelle *représentation linéaire* de G. Si le groupe des transformations linéaires G^{φ} est irréductible (resp. réductible, complètement réductible), on dit que φ est une *représentation irréductible* (resp. *réductible*, *complètement réductible*). Un homomorphisme ψ de G dans le groupe de matrices $\mathrm{GL}_n(K)$ s'appelle *représentation matricielle*. Les représentations φ et ψ sont intimement liées entre elles. C'est ainsi qu'à la représentation linéaire φ, dans une base donnée Σ de V, correspond la représentation matricielle φ_Σ, où g^{φ_Σ} est la matrice de la transformation linéaire g^{φ} dans la base Σ. En prenant une autre base Σ', on obtient une nouvelle représentation matricielle $\varphi_{\Sigma'}$ qui est équivalente à φ_Σ, i.e. liée à φ_Σ par la relation $g^{\varphi_{\Sigma'}} = tg^{\varphi_\Sigma}t^{-1}$, où t est la matrice de transition de Σ à Σ', $g \in G$.

20.2.1. Exemple. Soient G un groupe fini et A son sous-groupe normal décomposable en produit direct de n groupes cycliques d'ordre p. Introduisons sur A les opérations d'addition et de multiplication par les éléments du corps $\mathrm{GF}(p)$ de p éléments d'après les formules $a + b = ab$, $\alpha a = a^{\alpha}$, où l'exposant $\alpha \in \mathrm{GF}(p)$ est naturellement identifié à un nombre entier. On voit sans peine que A muni des opérations indiquées devient un espace vectoriel sur $\mathrm{GF}(p)$. Ensuite, la transformation $\hat{g}: x \mapsto x^g$, $g \in G$, $x \in A$, est une transformation linéaire de l'espace A, et la transformation $\hat{}$, un homomorphisme de G dans le groupe des transformations linéaires de A. On obtient ainsi une représentation linéaire de G, dans laquelle on a de toute évidence $\hat{G} \simeq G/C_G(A)$.

20.2.2. Théorème (Maschke). *Soit φ une représentation linéaire du groupe fini G par des transformations linéaires de l'espace vectoriel V sur le corps commutatif K. Si la caractéristique de K ne divise pas l'ordre de G, la représentation φ est complètement réductible.*

Démonstration. Etant donnée une représentation φ, supposons que G opère sur V. Soit U un sous-espace de V permis par G. Désignons par W un supplémentaire quelconque de U, i.e. $V = U \oplus W$. Désignons ensuite par π_W la projection de V sur le sous-espace W et posons

$$vt = \frac{1}{m} \sum_{g \in G} vg^{-1}\pi_W g, \quad v \in V,$$

où m est l'ordre du groupe G; l'application t est une transformation linéaire de l'espace V. En se donnant un $h \in G$, l'élément gh parcourt, en même temps que g, tous les éléments du groupe G. Il en découle les égalités

$$(vt)\,h = \frac{1}{m} \sum_g vh \cdot h^{-1} g^{-1} \pi_W g h = (vh)\,t$$

selon lesquelles le sous-espace linéaire $W_0 = Vt$ est permis par rapport à G.

Il reste à démontrer la décomposition $V = U \oplus W_0$. Prenons un élément quelconque $v \in V$ et mettons-le sous la forme d'une somme $v = (v - vt) + vt$, $vt \in W_0$. Le premier terme $v - vt$ de la somme est égal à

$$v - \frac{1}{m} \sum_g vg^{-1}\pi_W g = \frac{1}{m} \sum_g (vg^{-1} - vg^{-1}\pi_W)\,g.$$

Puisque $vg^{-1} - vg^{-1}\pi_W \in U$ et que U est permis, $v - vt$ appartient à U, d'où l'égalité $V = U + W_0$. Supposons enfin que $v \in U \cap W_0$. Puisque $v \in U$, le sous-espace U est permis par rapport à G et que, pour tout élément $u \in U$, la projection $u\pi_W$ est égale à 0, on a

$$vt = 0. \tag{1}$$

D'autre part, l'élément v appartient à W_0; il existe donc un élément $v' \in V$ tel que

$$v't = v. \tag{2}$$

Or, on a alors $vt = v't^2$. Nous avons indiqué plus haut que $v' - v't \in U$ et que par conséquent $v't - v't^2 = 0$. D'où l'égalité $vt = v't$ qui, jointe aux égalités (1), (2), entraîne $v = 0$. Le théorème est démontré.

20.2.3. Exemple. Soient G, A les mêmes que dans l'exemple 20.2.1. Il est évident qu'un sous-groupe $B \leqslant A$ est normal dans G si et seulement si le sous-espace vectoriel B de l'espace A est permis par rapport au groupe des transformations linéaires $\hat{G}$. Supposons que p ne divise pas l'ordre du groupe $G/C_G(A)$ et que B soit un sous-groupe normal de G contenu dans A. Puisque p ne divise pas l'ordre du groupe de transformations $\hat{G}$, le groupe $\hat{G}$ est complètement réductible en vertu du théorème de Maschke et, par conséquent, le sous-espace B admet un supplémentaire permis C. L'ensemble C est un sous-groupe normal du groupe G et $A = B \times C$.

20.2.4. Exercice (généralisation du théorème de Maschke). Soit G un groupe fini de transformations linéaires de l'espace vectoriel V sur un corps commutatif de caractéristique $p > 0$, et soit P

un p-sous-groupe de Sylow de G. Si le sous-espace G-permis U admet un supplémentaire P-permis, il admet aussi un supplémentaire G-permis.

Solution. Soit $V = U \oplus W$, où W est un sous-espace P-permis. Désignons par π_W la projection de V sur le sous-espace W et posons

$$vt = \frac{1}{m} \sum_{g \in S} vg^{-1}\pi_W g, \quad v \in V,$$

où $m = |G:P|$ et S est un ensemble d'éléments dont chacun provient d'une classe à droite de G suivant P. Il est clair que la projection π_W commute avec chaque élément du sous-groupe P. La transformation linéaire t ne dépend donc pas du choix de S. Pour démontrer que le sous-espace $W_0 = Vt$ est G-permis et que la décomposition $V = U \oplus W_0$ est valable, il suffit de reprendre à la lettre le raisonnement correspondant développé dans la démonstration du théorème de Maschke.

20.2.5. Exercice. Soit $A = B \times C$ un sous-groupe normal abélien de G tel que $(|A|, |G:A|) = 1$. Si B est normal dans G, il existe dans G un sous-groupe normal D tel que $A = B \times D$.

Le théorème de Maschke s'avère très utile pour la démonstration de l'importante proposition qui suit.

20.2.6. Théorème (Schur). *Soit G un groupe fini d'ordre n; supposons qu'il contient un sous-groupe normal A d'ordre k tel que $(k, l) = 1$, $l = n/k$. Le sous-groupe A admet alors au moins un supplémentaire, i.e. un sous-groupe B, tel que $G = A \cdot B$, $A \cap B = 1$.*

Démonstration. a) Supposons d'abord que A soit un groupe abélien de période p, où p est un nombre premier. En vertu du théorème de Frobenius 6.2.8, on peut admettre que G est un sous-groupe de l'entrelacement $W = A_{\wr} B$, $B = G/A$, et que

$$W = G \cdot \bar{A}, \quad G \cap \bar{A} = A, \text{ où } \bar{A} = \mathrm{Fun}\,(B, A)$$

(voir l'exercice 6.2.9). Puisque p ne divise pas $|G:A|$ et que $A \lhd W$, il existe dans W, en vertu du théorème de Maschke 20.2.2, un sous-groupe normal C tel que $\bar{A} = A \times C$. Des relations $W/C = \bar{A}/C \cdot BC/C$, $\bar{A} \cap BC = C$ et de l'isomorphisme canonique $\varphi: W/C \to G$ il découle que $G = AD$, où D est l'image de BC/C par φ.

b) Démontrons maintenant le théorème en levant les restrictions. On fera la démonstration en raisonnant par récurrence sur l'ordre du groupe. Supposons que le théorème soit faux pour le groupe G choisi, tout en restant vrai pour tout groupe d'ordre plus

petit. Remarquons que l'existence d'un supplémentaire de A est équivalente à l'existence dans G d'un sous-groupe d'ordre l, car $(k, l) = 1$.

Soient P un p-sous-groupe de Sylow dans A et $N(P)$ son normalisateur dans G. Puisque $G = A \cdot N(P)$, il existe dans $N(P)$ un sous-groupe normal $A \cap N(P)$ dont l'ordre est premier avec l'indice $l = |N(P) : A \cap N(P)|$. Si donc $|N(P)| < n$, par hypothèse de récurrence il existe dans le sous-groupe $N(P)$ et, partant, dans le groupe G un sous-groupe d'ordre l, ce qui est contradictoire avec le choix de G. Il s'ensuit que tout p-sous-groupe de Sylow de A est normal dans G, c'est pourquoi le commutant $A' < A$. Soit $A' \neq 1$. Le groupe G/A' vérifie alors les conditions du théorème et $|G : A'| < n$. Il existe donc dans G/A' un sous-groupe C/A' d'ordre l. L'hypothèse de récurrence appliquée au groupe C conduit à l'existence dans C d'un sous-groupe d'ordre l, ce qui contredit le choix de G, d'où la commutativité de A. Si ensuite $p \mid k$, $A^p \neq 1$, on retrouve la même contradiction en prenant $A^p = A'$. Le groupe A est donc abélien de période p. Compte tenu de a), le théorème est démontré.

Un complément essentiel du théorème de Schur est la proposition selon laquelle tous les sous-groupes d'ordre l sont conjugués deux à deux dans G. H. Zassenhaus a démontré cette proposition en stipulant la résolubilité du sous-groupe A, et S. A. Tchounikhine, celle du groupe quotient G/A. Or, en vertu du théorème de Feit-Thompson sur la résolubilité des groupes finis d'ordre impair (cf. le commencement du § 13), l'un au moins des groupes A, G/A est résoluble, ce qui fait que les supplémentaires dans le théorème de Schur sont toujours conjugués.

Avant de terminer ce n°, faisons quelques remarques générales concernant la réductibilité complète et l'irréductibilité.

20.2.7. Lemme. *Un groupe G de transformations linéaires d'un espace vectoriel V sur un corps commutatif K est complètement réductible si et seulement si V se décompose en somme directe de sous-espaces irréductibles permis.*

Démonstration. Supposons que G soit complètement réductible. Désignons par U_1 un sous-espace irréductible permis et supposons que soient construits des sous-espaces irréductibles permis $U_1, \ldots, U_s$ tels que $U \equiv (U_1, \ldots, U_s) = U_1 \oplus \ldots \oplus U_s$. Soit $U \neq V$. Il existe alors un supplémentaire permis W, $V = U \oplus W$, dans lequel on trouve un sous-espace irréductible permis U_{s+1}. De toute évidence la somme $U + U_{s+1}$ est directe, et un raisonnement par récurrence achève la démonstration.

Soit réciproquement $V = U_1 \oplus \ldots \oplus U_r$, $U_i G \leqslant U_i$, où U_i est un sous-espace irréductible. Prenons un sous-espace permis quelconque U, désignons par I une partie maximale de l'ensemble

d'indices $\{1, 2, \ldots, r\}$ telle que $U \cap \sum_{i \in I} U_i = 0$ et montrons que $V = U \oplus \sum_{i \in I} U_i$. En effet, s'il n'en est pas ainsi, il existe un j tel que $U_j \cap (U \oplus \sum_{i \in I} U_i) = 0$. Or, on a alors

$$U \cap (U_j \oplus \sum_{i \in I} U_i) = 0,$$

ce qui est contradictoire avec le choix de I.

20.2.8. Exercice. Un groupe de transformations linéaires d'un espace V est complètement réductible si et seulement si tout sous-espace irréductible permis admet un supplémentaire permis.

20.2.9. Lemme. *Toute représentation irréductible d'un groupe abélien G sur un corps commutatif algébriquement clos est de dimension* 1.

Démonstration. Supposons que le groupe G opère irréductiblement dans un espace V sur un corps commutatif algébriquement clos K. Si $g \in G$, λ est le nombre caractéristique de la transformation linéaire g et $vg = \lambda v$, $0 \neq v \in V$, il ressort de $(vf)\, g = (vg)\, f = \lambda\, (vf)$, $f \in G$, que l'ensemble U des vecteurs propres de g correspondant à λ est un sous-espace permis. Le groupe G étant irréductible, on a $V = U$. Ainsi donc, tout vecteur non nul dans V est un vecteur propre pour tout $g \in G$. D'où, en se rappelant que G est irréductible, on déduit que V est de dimension 1.

20.3. Critère d'hyperrésolubilité. Nous établirons ici un

20.3.1. Théorème (Huppert). *Un groupe fini est hyperrésoluble si et seulement si tous ses sous-groupes maximaux ont les indices premiers.*

Démonstration. La condition est nécessaire. Supposons que G soit un groupe fini hyperrésoluble et, par récurrence sur $|G|$, montrons que ses sous-groupes maximaux ont les indices premiers.

Puisque G est hyperrésoluble, il admet un sous-groupe normal N d'ordre p, où p est un nombre premier. Si maintenant M est un sous-groupe maximal dans G, on a $M \cap N = 1$ ou $N \leqslant M$. Dans le premier cas, l'indice de M dans G est visiblement p. Dans le deuxième cas, le sous-groupe M/N est maximal dans G/N et, par hypothèse de récurrence, est d'indice premier. Il en découle que M est d'indice premier dans G.

La condition est suffisante. Supposons que les sous-groupes maximaux de G aient les indices premiers, et supposons

démontré que tous les groupes de ce type d'ordres inférieurs à $|G|$ sont hyperrésolubles. Démontrons d'abord la résolubilité de G. Désignons par p le plus grand diviseur premier de l'ordre $|G|$ et par M' un sous-groupe maximal quelconque contenant un p-sous-groupe de Sylow de G. Alors $|G : M'| < p$ et, conformément à l'exercice 11.3.6, l'intersection $M'' = \bigcap_{g \in G} M'^g$ est non triviale et certainement normale dans G. Il existe donc dans G un sous-groupe normal minimal M distinct de G. Prenons un q-sous-groupe de Sylow Q dans M, où q est le plus grand diviseur premier de l'ordre $|M|$, et supposons que son normalisateur $N(Q)$ soit distinct de G. Puisque $N(Q)M = G$ (lemme de Frattini 17.1.8), on a *a fortiori* $HM = G$, où H est un sous-groupe maximal quelconque de G, $H \geqslant N(Q)$, d'où $|G : H| = |M : M \cap H|$. L'indice premier $|M : M \cap H| = q'$ divise le nombre $|M : N_M(Q)|$ qui est premier avec q, d'où $q' < q$. Toujours en accord avec l'exercice 11.3.6, on est en droit d'affirmer qu'il existe dans M un sous-groupe normal propre M_0 qui contient tous les q-éléments de M. La même propriété reste vraie pour tout sous-groupe conjugué de M_0. Aussi, l'intersection $\bigcap_{g \in G} M_0^g$ est-elle non triviale, distincte de M et normale dans G, ce qui est contradictoire avec le choix de M. De cette contradiction il découle que $N(Q) = G$, i.e. $Q \trianglelefteq G$ et donc $Q = M$. Il existe donc dans G un sous-groupe normal résoluble M tel que le groupe quotient de G par M est hyperrésoluble par hypothèse de récurrence. Il s'ensuit que G est résoluble.

Nous savons que tout sous-groupe normal minimal M d'un groupe résoluble G est abélien et se décompose en produit direct de groupes cycliques d'ordre q premier (exercice 19.1.7). Il reste à montrer que $|M| = q$, ou au moins qu'il existe dans G un sous-groupe normal cyclique. Deux possibilités sont à distinguer ici :

1° Le plus grand diviseur premier p de l'ordre du groupe G est strictement supérieur à q. Il existe alors dans G/M un sous-groupe normal A/M d'ordre p (théorème 19.2.3). Si $N(P) = G$, où $P < A$ est un sous-groupe d'ordre p, il existe dans G un sous-groupe normal cyclique, d'où il découle que G est hyperrésoluble. Si au contraire $N(P) \neq G$, le sous-groupe maximal $H \geqslant N(P)$ ne contient pas M (sinon, il y aurait $G = N(P)A = HPM \leqslant H$), d'où $G = HM$ et l'intersection $H \cap M$ est normale dans G. Comme M est minimal, l'intersection en question est triviale et, puisque l'indice $|G : H|$ est premier, l'ordre de M est égal à q, ce qu'il fallait démontrer.

2° Le plus grand diviseur premier de l'ordre de G est égal à q. Comme le groupe G/M est hyperrésoluble et en vertu du théorème 19.2.6, le q-sous-groupe de Sylow G_q est alors normal dans G. Puisque le centre Z de G_q est normal dans G et que $Z \cap M \neq 1$ (cf. le théorème 16.2.3), on a $M \leqslant Z$.

Si $M = G_q$, il existe dans le groupe quotient G/M un sous-groupe normal A/M d'ordre p premier et distinct de q. L'hyperrésolubilité de G se démontre alors de la même façon que dans l'éventualité 1°.

Soit maintenant $M \neq G_q$. Désignons par B/M un sous-groupe normal d'ordre q dans G/M. Il est évident que B est un sous-groupe abélien. Tous les éléments de B sont d'ordre q, sinon B^q serait le sous-groupe cherché d'ordre q, normal dans G.

Supposons d'abord que B n'est pas contenu dans le centre Z. Il va sans dire que les éléments de B appartiennent au deuxième hypercentre du groupe G_q. Puisque le groupe G/B est hyperrésoluble, il existe une matriochka

$$1 < B = B_0 < B_1 < \ldots < B_s = G_q$$

telle que $B_i \trianglelefteq G$, $|B_{i+1} : B_i| = q$. Il existe un k tel que $B \leqslant Z(B_k)$ mais que $B \not\leqslant Z(B_{k+1})$. Soit $B = (M, b)$, $B_{k+1} = (B_k, b_{k+1})$. L'ensemble de tous les éléments de la forme $[b, x]$, $x \in B_{k+1}$, est alors un sous-groupe d'ordre q, normal dans G. En effet, pour des éléments quelconques $x = c_1 b_{k+1}^l$, $y = c_2 b_{k+1}^m$, $c_1, c_2 \in B_k$, $g \in G$, on a

$$[b, x][b, y] = [b, b_{k+1}^l][b, b_{k+1}^m] = [b, b_{k+1}]^{l+m},$$

$$[b, b_{k+1}]^g = [b^g, b_{k+1}^g] = [ab^n, c_3 b_{k+1}^r] = [b, b_{k+1}]^{n+r},$$

où a, c_3 sont des éléments de M et de B_k respectivement.

On peut donc admettre que B est contenu dans le centre du groupe G_q. Par ailleurs, B peut être assimilé à un espace vectoriel sur le corps $\mathrm{GF}(q)$, et le groupe F des automorphismes de B induits par les automorphismes intérieurs du groupe G, à un groupe de transformations linéaires de cet espace (cf. l'exemple 20.2.1). Puisque $B \leqslant Z$, l'ordre du groupe F isomorphe à $G/C_G(B)$ est premier avec q. En vertu du théorème de Maschke 20.2.2, il en découle que le sous-espace M permis par rapport à F admet dans B un supplémentaire permis A de dimension 1. Traduit dans le langage des groupes, ce résultat signifie que A est un sous-groupe normal cyclique du groupe G.

Dans chacune des éventualités envisagées, le groupe G admet donc un sous-groupe normal d'ordre premier. Comme nous l'avons dit plus haut, cela achève la démonstration du théorème.

20.3.2. Exercice. Un groupe fini est hyperrésoluble si et seulement si son groupe quotient par le sous-groupe de Frattini est hyperrésoluble.

§ 21. Groupes de matrices résolubles

Au commencement de ce chapitre, nous avons mentionné les groupes matriciels trigonaux à titre d'exemple de groupes résolubles (exercice 19.1.2). Un autre exemple de groupe matriciel résoluble

est donné, au fond, par n'importe quel groupe résoluble fini, car, en vertu du théorème de Cayley 12.1.1, un tel groupe est représentable par des permutations, donc aussi par des matrices. Réunissant ces exemples, nous pouvons considérer la classe des extensions des groupes matriciels trigonaux par des groupes résolubles finis: conformément à l'exercice 17.2.7, toutes ces extensions sont représentables par des matrices. Il se trouve que cette classe contient tout groupe de matrices résoluble sur un corps algébriquement clos, car le groupe en question est presque trigonal à conjugaison près dans le groupe linéaire général. Ce résultat, résumé dans le théorème de Koltchine-Maltsev, sera établi dans le premier n° du présent paragraphe. Dans le deuxième n° nous examinerons les sous-groupes résolubles de $\mathrm{GL}_n(\mathbb{Z})$ pour montrer qu'ils sont tous polycycliques. Enfin, dans le troisième n° nous montrerons que l'holomorphe d'un groupe polycyclique quelconque admet une image isomorphe dans $\mathrm{GL}_n(\mathbb{Z})$ pour un certain n.

21.1. La presque trigonalisabilité. On dit d'un groupe de matrices $H \leqslant \mathrm{GL}_n(K)$ qu'il est *trigonalisable* si pour un $g \in \mathrm{GL}_n(K)$ le groupe H^g est trigonal. Avant de montrer que les groupes matriciels résolubles sont presque trigonalisables, considérons les propriétés générales des groupes matriciels irréductibles et complètement réductibles (les définitions et les propriétés élémentaires sont données dans le n° 20.2). Ce faisant, nous assimilerons le plus souvent le groupe de matrices G à un groupe de transformations linéaires d'un espace dont les matrices se confondent, dans une base donnée, avec les éléments de G.

21.1.1. Lemme (Clifford). *Tout sous-groupe normal H d'un groupe complètement réductible G de transformations linéaires d'un espace vectoriel V est lui-même complètement réductible.*

Démonstration. Soit U_1 un sous-espace irréductible permis par rapport à H. Il existe alors un ensemble minimal d'éléments $g_1, \ldots, g_s$ du groupe G tel que la clôture G-permise $\overline{U}_1$ de U_1 soit engendrée par les sous-espaces $U_i \equiv U_1 g_i$, $i = 1, \ldots, s$. On voit sans peine que les U_i sont H-permis et que $\overline{U}_1 = U_1 \oplus \ldots \oplus U_s$. Pour $\overline{U}_1 \neq V$ il existe un supplémentaire permis B dans lequel on trouve un sous-espace U' irréductible permis par rapport à H. Par analogie à $\overline{U}_1$, construisons $\overline{U}_2 = U_{s+1} \oplus \ldots \oplus U_k \leqslant B$. Il est évident que $\overline{U}_1 \oplus \overline{U}_2 = U_1 \oplus \ldots \oplus U_k$. En poursuivant ce raisonnement, on montre que V se décompose en somme directe de sous-espaces irréductibles permis par rapport à H. Compte tenu du lemme 20.2.7, cela achève la démonstration.

21.1.2. L e m m e. *Le centre d'un groupe de matrices irréductible sur un corps commutatif algébriquement clos est constitué de matrices scalaires.*

D é m o n s t r a t i o n. Supposons que G opère irréductiblement dans un espace vectoriel V sur un corps commutatif algébriquement clos. En vertu du lemme de Clifford, son centre Z est complètement réductible; l'espace V admet donc une base $v_1, \ldots, v_n$ constituée de vecteurs propres des éléments de Z (voir le lemme 20.2.9). Soient $c \in Z$, $v_i c = \lambda_i v_i$ et par exemple $\lambda_1 \neq \lambda_2$. Désignons par U le sous-espace engendré par les v_i tels que $\lambda_i = \lambda_1$. Le sous-espace U est permis (propre). En effet, quel que soit $g \in G$, le vecteur $v_1 g$ se laisse mettre sous la forme $v_1 g = \alpha_1 v_1 + \ldots + \alpha_n v_n$. Des égalités

$$v_1 (gc) = \alpha_1 \lambda_1 v_1 + \ldots + \alpha_n \lambda_n v_n,$$
$$v_1 (cg) = \lambda_1 (\alpha_1 v_1 + \ldots + \alpha_n v_n)$$

et de l'égalité $gc = cg$ on obtient $\alpha_j = 0$ pour $\lambda_j \neq \lambda_1$, d'où $v_1 g \in U$. Il va sans dire que la relation $v_i g \in U$ est valable pour tout $v_i \in U$. Nous venons de montrer donc que U est permis, ce qui est contradictoire avec l'irréductibilité du groupe G. De cette contradiction il ressort que $\lambda_1 = \lambda_j$, $j = 1, 2, \ldots, n$.

Avec le lemme suivant, nous pourrons opérer par récurrence sur l'ordre des matrices.

21.1.3. L e m m e. *Soit G un groupe irréductible de matrices d'ordre n sur un corps commutatif algébriquement clos. Supposons qu'il existe dans G un sous-groupe normal abélien non central H. Il existe alors dans G un sous-groupe normal réductible d'indice fini $\leqslant (n!)!$.*

D é m o n s t r a t i o n. En vertu du lemme de Clifford 21.1.1, le sous-groupe H est complètement réductible. On peut donc admettre, conformément aux lemmes 20.2.7 et 20.2.9, que H est diagonal. Puisque H n'est pas inclus dans le centre de G, il existe une matrice non scalaire $b \in H$. Pour tout $g \in G$, l'élément b^g appartient à H et admet les mêmes nombres caractéristiques que b. On a donc $|b^G| \leqslant n!$. L'application $G \to S(b^G)$ définie par

$$g \mapsto \begin{pmatrix} b^x \\ b^{xg} \end{pmatrix}$$

est un homomorphisme. Son noyau A est évidemment contenu dans $C_G(b)$ et $|G : A| \leqslant (n!)!$. Le centre A contient la matrice non scalaire b, aussi le groupe A est-il réductible en vertu du lemme 21.1.2.

21.1.4. Lemme. *Si G admet un sous-groupe normal abélien A d'indice n, il existe dans G un sous-groupe abélien Aut-permis d'indice fini non supérieur à un nombre qui ne dépend que de n.*

Démonstration. De toute évidence, il existe des sous-groupes Aut-conjugués de A, $A = A_1, A_2, \ldots, A_s$, $s \leqslant n$, tels que $S = \mathrm{gr}\,(A_1, \ldots, A_s)$ se confond avec le sous-groupe engendré par tous les sous-groupes Aut-conjugués de A. Le sous-groupe S est Aut-permis. Son centre Z contient $\bigcap A_i$, aussi l'indice $|G:Z|$ est-il non supérieur à n^n. Le sous-groupe Z est précisément celui dont il s'agit dans le lemme.

Maintenant nous avons réuni presque tous les éléments nécessaires pour la démonstration du théorème de Koltchine-Maltsev. En plus de ceux-ci, nous aurons besoin de l'exercice 27.3.2 de l'Appendice, qui nécessite l'emploi direct d'un théorème local de la logique. Nous proposons au lecteur d'admettre provisoirement le résultat de l'exercice sans preuve, les théorèmes locaux faisant l'objet d'un n° spécial dans le § 22. Le lecteur peut aussi essayer de résoudre directement l'exercice en question.

21.1.5. Théorème (Koltchine-Maltsev). *Tout groupe résoluble G de matrices d'ordre n sur un corps commutatif algébriquement clos admet un sous-groupe trigonalisable d'indice fini non supérieur à un nombre, qui ne dépend que de n.*

Démonstration. a) Supposons d'abord que G soit irréductible et nilpotent. En vertu du lemme 20.2.9, il suffit de montrer que G admet un sous-groupe normal abélien d'indice fini non supérieur à un nombre $\tau\,(n)$ qui ne dépend que de n. Nous le ferons par récurrence sur n.

Si G est non abélien, il existe dans G un sous-groupe normal abélien non central (par exemple, n'importe quel sous-groupe normal abélien maximal, cf. le théorème 16.2.6). En vertu du lemme 21.1.3, le groupe G admet alors un sous-groupe normal réductible H d'indice fini $\leqslant (n!)!$. D'après le lemme de Clifford 21.1.1, le groupe H est complètement réductible, donc décomposable en produit sous-direct de groupes nilpotents irréductibles H_i dont les degrés sont inférieurs à n. Par hypothèse de récurrence, il existe dans chaque H_i un sous-groupe normal abélien d'indice fini non supérieur à $\tau\,(n - 1)$. Or, il existe alors dans H un sous-groupe normal abélien A d'indice $< \tau\,(n-1)^n$. Puisque $|G:A| < (n!)!\ \tau\,(n-1)^n$, l'intersection B des sous-groupes conjugués de A prend dans G un indice non supérieur à un nombre que l'on peut retenir comme $\tau\,(n)$.

b) Supposons que le groupe G soit irréductible et résoluble, sans demander qu'il soit nilpotent comme précédemment. Montrons par récurrence sur n que G admet comme précédemment un sous-groupe

normal abélien d'indice fini non supérieur à un nombre $\rho(n)$ qui ne dépend que de n.

Si G admet au moins un sous-groupe normal abélien non central, la démonstration de a) peut être reprise à la lettre. Supposons donc que tous les sous-groupes normaux abéliens de G soient centraux. Désignons par R le sous-groupe engendré par tous les sous-groupes normaux nilpotents de G. En vertu de a) et de l'exercice 27.3.2 de l'Appendice, il existe dans R un sous-groupe normal abélien d'indice fini $\leqslant \tau_0(n)$. Suivant le lemme 21.1.4, il existe dans R un sous-groupe abélien Aut-permis B d'indice fini $\leqslant \tau_1(n)$, où τ_1 est une fonction. Remarquons que R est nilpotent et que B est contenu dans le centre de G. Estimons l'indice $|G:R|$.

Soit $1 < B = B_0 < B_1 < \ldots < B_s = R$ une matriochka centrale de sous-groupes Aut-permis de R. Soit Z le centralisateur de cette matriochka dans G, i.e. $Z = \bigcap Z_i$, où Z_{i+1}/B_i est le centralisateur de la section B_{i+1}/B_i dans G/B_i. Il est clair que $R \leqslant Z$. Si $R < Z$ et A/R est un sous-groupe abélien Aut-permis non trivial dans Z/R, alors A est un sous-groupe normal nilpotent de G qui contient strictement R, ce qui est impossible. On a donc $Z = R$. Puisque $B \leqslant Z(G)$ et $|R:B| \leqslant \tau_1(n)$, on a $|G:R| \leqslant \tau_2(n)$, où τ_2 est une fonction. On peut donc prendre $\rho(n) = \tau_1(n)\,\tau_2(n)$, si bien que B est le sous-groupe cherché.

c) Plaçons-nous enfin dans le cas général. Soit V un espace muni d'une base $e_1, \ldots, e_n$; supposons que G opère sur V. Prenons une matriochka non subdivisible

$$V = V_1 > V_2 > \ldots > V_{s+1} = 0 \tag{1}$$

de sous-espaces G-permis. Le groupe G opère irréductiblement sur chaque section V_i/V_{i+1}. En vertu de b), il existe dans G des sous-groupes normaux G_i tels que $|G:G_i| \leqslant \rho(n)$ et que le groupe G_i/A_i est abélien (on désigne par A_i le noyau de la représentation de G induite dans V_i/V_{i+1}). Posons $G_0 = \bigcap_i G_i$. En vertu du lemme 20.2.9, il est possible de subdiviser la matriochka (1) de façon à obtenir une matriochka G_0-permise

$$V = V'_n > V'_2 > \ldots > V'_{n+1} = 0$$

à sections de dimension 1. Les matrices des transformations linéaires appartenant à G_0 sont trigonales dans la base $f_1, \ldots, f_n$, $f_j \in V'_j \setminus V'_{j+1}$. Par conséquent, le sous-groupe G_0 se laisse trigonaliser par conjugaison à l'aide de la matrice de transition de $\{f_j\}$ à $\{e_i\}$. Il est évident que l'indice de G_0 est non supérieur à un nombre qui ne dépend que de n. Le théorème est démontré.

21.1.6. Exercice. Le degré de résolubilité d'un groupe résoluble quelconque de matrices d'ordre n de dépasse pas un nombre qui ne dépend que de n. En déduire qu'un groupe de matrices dont

tous les sous-groupes de type fini sont résolubles est lui-même résoluble.

21.1.7. Exercice. Tout groupe résoluble de matrices d'ordre n admet un sous-groupe normal dont le commutant est nilpotent et l'indice non supérieur à un nombre qui ne dépend que de n. Ce résultat s'avère souvent utile quand il s'agit de montrer que tel ou tel groupe abstrait ne peut être représenté par des matrices (voir par exemple D. M. Smirnov in: *Matem. sb.*, 1965, 67, n° 3, p. 366-383).

21.2. Polycyclicité des groupes résolubles de $GL_n(\mathbb{Z})$. Soit $\overline{\mathbb{Q}}$ la clôture algébrique du corps $\mathbb{Q}$ des nombres rationnels. Les éléments de $\overline{\mathbb{Q}}$ s'appellent *nombres algébriques*. On dit qu'un élément de $\overline{\mathbb{Q}}$ est un *entier algébrique* s'il est racine d'un polynôme à coefficients entiers dont le coefficient dominant est 1.

Soit K un corps de nombres algébriques de degré fini sur $\mathbb{Q}$. En vertu du § 28 de l'Appendice, l'ensemble k de tous les entiers algébriques de K est un anneau dont les groupes additif et multiplicatif sont de type fini. Ces résultats de la théorie des nombres vont être utilisés pour démontrer un

21.2.1. Théorème (A. I. Maltsev). *Tout groupe résoluble de matrices entières est polycyclique.*

Démonstration. Soit G un groupe résoluble de matrices entières d'ordre n. En vertu du théorème de Koltchine-Maltsev 21.1.5, il existe une matrice $g = (g_{ij})$ et un sous-groupe $A \leqslant G$ d'indice fini tels que $B = A^g$ est contenu dans le groupe des matrices trigonales $T_n(K)$ sur l'extension algébrique

$$K = \mathbb{Q}(g_{11}, g_{12}, \ldots, g_{nn})$$

du corps $\mathbb{Q}$. Il est clair que tout élément g_{ij} peut être assimilé à un entier dans K. Il s'ensuit que tout élément d'une matrice de B se laisse mettre sous la forme d'une fraction dont le numérateur est un entier algébrique et le dénominateur est égal au déterminant de la matrice g. Soient k l'anneau de tous les entiers algébriques de K, et k^* le groupe multiplicatif de k. Les éléments diagonaux des matrices de B vérifient les équations caractéristiques des matrices de A, dont les coefficients dominants sont égaux à 1 : les éléments diagonaux en question appartiennent donc à k^*. Considérons l'homomorphisme $B \to k^* \times \ldots \times k^*$ (n fois) qui à toute matrice $b \in B$ fait correspondre sa diagonale. Soit C le noyau de cet homomorphisme. En vertu du théorème 28.1.12 de l'Appendice, le groupe quotient B/C est de type fini. Le noyau C réunit toutes les matrices unitrigonales de B. Désignons par C_i le sous-groupe de toutes les matrices

de C qui présentent i diagonales nulles au-dessus de la principale. Il est clair que la matriochka

$$C = C_0 \geqslant C_1 \geqslant \ldots \geqslant C_{n-1} = 1$$

est une matriochka normale dans C. On voit sans peine que chaque section C_i/C_{i+1} est isomorphe à un sous-groupe de la somme directe de $n - i - 1$ copies du groupe additif de l'anneau k, le groupe indiqué étant de type fini en vertu du théorème 28.1.6 de l'Appendice. Il s'ensuit que C est de type fini ; par conséquent, il en est de même pour B. Puisque $B = A^g$ et que l'indice $|G : A|$ est fini, le groupe G tout entier est de type fini. Il est clair que cela achève la démonstration du théorème.

Le théorème que nous venons de démontrer conduit à une proposition moins restrictive :

21.2.2. Théorème. *Tout groupe résoluble d'automorphismes d'un groupe abélien de type fini est polycyclique.*

Démonstration. Soient A un groupe abélien de type fini et Φ un groupe résoluble d'automorphismes de A. Désignons par Φ la partie périodique de A et considérons l'homomorphisme τ : $H \to \mathrm{Aut}\,(A/H)$ qui à tout $\varphi \in \Phi$ fait correspondre l'automorphisme $\bar{\varphi}$ du groupe quotient A/H induit par φ, i.e. $(Ha)^{\bar{\varphi}} = Ha^{\varphi}$. En vertu du théorème précédent, le groupe quotient Φ/Ψ, où $\Psi = \ker \tau$, est de type fini. Montrons que Ψ est fini. En effet, si $a_1, \ldots, a_n$ est un système de générateurs de A, pour tout $\psi \in \Psi$ on a $a_i^{\psi} = h_i a_i$, $h_i \in H$. Puisque la partie périodique H est finie, il n'existe qu'un nombre fini de possibilités pour les images des générateurs a_i par les applications de Ψ. Il s'ensuit que Ψ est fini et que, par conséquent, Φ est de type fini. On voit maintenant que Φ est un groupe polycyclique, ce qu'il fallait démontrer.

21.3. Les holomorphes des groupes polycycliques se plongent dans $\mathrm{GL}_n(\mathbb{Z})$. Soit G un groupe. On voit sans peine qu'on obtient l'action de son holomorphe $\mathrm{Hol}\, G$ sur l'anneau de groupe entier $\mathbb{Z}[G]$ en posant

$$\left(\sum \alpha_i g_i\right)^{\varphi g} = \sum \alpha_i g_i^{\varphi} g, \quad \alpha_i \in \mathbb{Z}, \quad \varphi \in \mathrm{Aut}\, G, \quad g_i, g \in G. \qquad (2)$$

21.3.1. Lemme. *Soient $G \leqslant \mathrm{GL}_n(\mathbb{Z})$, N un sous-groupe normal unitrigonal de G, et G/N le groupe quotient de type fini. Si Φ est un sous-groupe de* Aut G *qui envoie N dans lui-même et opère identiquement dans G/N, il existe un entier naturel m et un homomorphisme injectif $\Phi G \to \mathrm{GL}_m(\mathbb{Z})$ unitrigonal sur N.*

Démonstration. Prolongeons l'injection canonique définie par $G \leqslant \mathrm{GL}_n(\mathbb{Z})$ en homomorphisme d'anneaux $\rho : \mathbb{Z}[G] \to$

$\to \mathbf{M}_n(\mathbb{Z})$; soit K son noyau. Soit I l'idéal de l'anneau $\mathbb{Z}[G]$ engendré par toutes les différences $1 - x$, $x \in N$. Puisque le groupe N est unitrigonal, on a

$$((1 - x_1) \ldots (1 - x_n))^p = 0 \quad \text{pour } x_i \in N,$$

d'où $I^n \subset K$ et, par conséquent, $(I + K)^n \subset K$. En vertu du théorème 26.1.4 de l'Appendice, le groupe additif $\mathbb{Z}[G]/(I + K)^n$ est de type fini. Soit $T/(I + K)^n$ sa partie périodique. Puisque le groupe additif $\mathbb{Z}[G]/K$ est sans torsion, on a $T \subset K$. Par définition, pour tous $\varphi \in \Phi$, $g \in G$ on a $g^\varphi = gx$, $x \in N$, donc $g^\varphi - g = g(x - 1) \in I$. On voit que le groupe additif $I + K$ est ΦG-permis. L'action de ΦG sur $\mathbb{Z}[G]$ induit donc, en vertu de (2), celle de ΦG sur le groupe additif de type fini $\mathbb{Z}[G]/T$. Elle est fidèle, car $T \subset K$. Il reste à vérifier que N opère sur $\mathbb{Z}[G]/T$ de façon unitrigonale. Par hypothèse de récurrence, il suffit de trouver dans $\mathbb{Z}[G]/T$ un élément N-invariant non nul. Puisque $I^n \subset T$, il existe un $s \geqslant 0$ tel que $I^s \not\subset T$, $I^{s+1} \subset T$ (nous admettons que $I^0 = \mathbb{Z}[G]$). Tout élément de $I^s \setminus T$ modulo T est non nul et N-invariant. Le lemme est démontré.

21.3.2. Théorème (Iou. I. Merzliakov). *L'holomorphe* Hol G *d'un groupe polycyclique quelconque* G *admet une image isomorphe dans* $\mathbf{GL}_n(\mathbb{Z})$ *pour un certain* n.

Démonstration. a) Le groupe G admet une matriochka Aut-permise $G \geqslant M \geqslant N \geqslant 1$, où $|G : M| < \infty$, M est un groupe sans torsion, M/N un groupe abélien sans torsion, N un sous-groupe normal nilpotent maximal dans M. En effet, prenons dans G une matriochka normale $G = G_1 > G_2 > \ldots > G_{l+1} = 1$ dont chaque section est soit apériodique, soit périodique de période première. Le groupe G opère dans ces sections par conjugaisons, ce qui définit des représentations matricielles $\varphi_i : G \to \mathrm{Aut}\,(G_i/G_{i+1})$ par rapport à des bases données dans les sections G_i/G_{i+1}. Si i est tel que G_i/G_{i+1} est sans torsion, le groupe G^{φ_i} contient, en vertu du théorème de Koltchine-Maltsev 21.1.5, un sous-groupe S_i d'indice fini, trigonalisable dans $\mathbf{GL}_{n_i}(\mathbb{C})$, où n_i est la dimension de la section G_i/G_{i+1}; soit alors T_i l'image réciproque du groupe $S_i^{\varphi_i}$ dans G. Si par contre G_i/G_{i+1} est périodique de période première, posons $T_i = \mathrm{Ker}\,\varphi_i$. L'intersection $T = \bigcap T_i$ est d'indice fini dans G et opère de façon trigonale dans toutes les sections. Compte tenu de l'exercice 17.2.3, on peut admettre que T est sans torsion. Puisque le commutant T' opère de façon unitrigonale, on a $[G_i, T', \ldots, T'] \leqslant G_{i+1}$. On a donc $[G, T', \ldots, T'] = 1$, à condition que le nombre de commutations soit suffisamment grand. En particulier, le groupe T' est nilpotent. Nous savons que tout sous-groupe d'indice fini dans un groupe de type fini contient un sous-groupe verbal d'indice fini

(exercice 15.2.3). Soit V un sous-groupe verbal dans G tel que $V \leqslant T$, $|G:V| < \infty$, et soit N un sous-groupe normal nilpotent maximal dans V. Puisque $V' \leqslant T' \cap V \leqslant N$, le groupe V/N est abélien. Soit m la période de sa partie périodique. Posons $M = V^m N$. Il est clair que M, N sont les groupes que l'on cherche.

b) Soit Φ le groupe de tous les automorphismes de M qui opèrent identiquement sur M/N. Montrons qu'il existe une représentation isomorphe de ΦM par matrices sur $\mathbb{Z}$, qui est unitrigonale sur N. Tout d'abord, démontrons-le pour M en raisonnant par récurrence sur le degré r du groupe abélien libre M/N. Si $r = 0$, la proposition résulte du théorème 17.2.5. Soient

$$M = (a)\cdot M_0, \quad (a) \cap M_0 = 1, \quad N \leqslant M_0 \lhd M$$

et le degré de M_0/N égal à $r - 1$. Par hypothèse de récurrence, on peut admettre que M_0 possède la représentation demandée. En vertu du lemme 21.3.1, on conclut alors que M admet, lui aussi, une telle représentation. Appliquant ce lemme une fois de plus, on voit que ΦM admet cette représentation à son tour.

c) L'holomorphe Hol M est représentable de façon isomorphe par des matrices sur $\mathbb{Z}$. En effet, compte tenu de b) et de l'exercice 17.2.7, il suffit de s'assurer que $|\operatorname{Aut} M : \Phi| < \infty$. C'est ce que nous allons vérifier tout de suite. Tout d'abord, la commutativité de M/N et les relations entre commutateurs citées dans le n° 3.2 font qu'on a dans Hol M

$$[M/N, \alpha]^m \leqslant [(M/N)^m, \alpha] \leqslant [M^m, \alpha]\, N/N \tag{3}$$

pour tous $\alpha \in \operatorname{Aut} M$, $m = 1, 2, \ldots$ Soit $\beta \in \operatorname{Aut} M$. Puisque le sous-groupe $(\beta)\, M$ de l'holomorphe Hol M est polycyclique, il contient un sous-groupe normal T d'indice fini m dont le commutant T' est nilpotent (voir a)). Puisque N est un sous-groupe normal nilpotent maximal dans M, on a

$$[M^m, \beta^m] \leqslant T' \cap M \leqslant N.$$

Compte tenu de ce résultat, il ressort de (3) que $[M/N, \beta^m]^m = 1$. Puisque M/N est sans torsion, on a $[M/N, \beta^m] = 1$, i.e. $\beta^m \in \Phi$. Ainsi donc, le groupe $(\operatorname{Aut} M)/\Phi$ est périodique. Si r est le rang de M/N, on obtient un homomorphisme injectif évident $(\operatorname{Aut} M)/\Phi \to \mathbf{GL}_r(\mathbb{Z})$. Puisque $\mathbf{GL}_r(\mathbb{Z})$ est presque sans torsion (voir les exercices 4.2.7 et 5.1.5), le groupe $(\operatorname{Aut} M)/\Phi$ est fini.

d) L'holomorphe Hol G est représentable à isomorphisme près par des matrices sur $\mathbb{Z}$. On sait en effet qu'il existe pour tout groupe X une injection

$$\operatorname{Hol} X \to \operatorname{Aut}(X \wr \mathbb{Z}_2). \tag{4}$$

Pour obtenir cette injection, posons que Hol X opère sur $X \wr \mathbb{Z}_2$ de façon à avoir

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^{\varphi g} = \begin{pmatrix} x^{\varphi g} & 0 \\ 0 & y^{\varphi} \end{pmatrix}, \quad \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}^{\varphi g} = \begin{pmatrix} 0 & g^{-1}x^{\varphi} \\ y^{\varphi}g & 0 \end{pmatrix} \tag{5}$$

pour tous $\varphi \in \operatorname{Aut} X$, x, y, $g \in X$. Toutes les propriétés requises sont faciles à vérifier. Si X est un groupe polycyclique, il en est visiblement de même pour $X \wr \mathbb{Z}_2$; au lieu de Hol G, il suffit donc de représenter par matrices le groupe Aut G. Soit ensuite Γ le groupe de tous les automorphismes de G qui opèrent identiquement dans une section (finie) G/M. Puisque $|\operatorname{Aut} G : \Gamma| < \infty$, il suffit de représenter Γ. Soit S un ensemble fini qui engendre G modulo M. Considérons l'application $\Gamma \to \operatorname{Hol} M \times \ldots \times \operatorname{Hol} M$ définie par

$$\gamma \mapsto \prod_{s \in S} \gamma|_M \cdot [\gamma, s]. \tag{6}$$

On voit immédiatement que c'est un homomorphisme injectif. Puisque Hol M se laisse représenter à isomorphisme près par des matrices sur $\mathbb{Z}$ (voir c)), il en est de même pour Γ. Le théorème est démontré.

21.3.3. Exercice. Si M est un sous-groupe Aut-permis d'indice fini dans un groupe G et si Hol M est représentable à isomorphisme près par des matrices, Hol G est à son tour représentable par des matrices à isomorphisme près.

21.3.4. Exercice. L'holomorphe de tout groupe polycyclique est presque sans torsion et, pour tout p premier, admet presque une approximation par des p-groupes finis.

Indication. Voir la démonstration du théorème 14.2.2.

Le rôle du théorème 21.3.2 consiste à ouvrir la voie vers la théorie des groupes polycycliques aux méthodes de la géométrie algébrique, de la théorie des nombres et de l'analyse p-adique, en fonction du choix de l'anneau principal des coefficients sous-jacent à $\mathbb{Z}$. Par exemple, Wehrfritz a remarqué que ce théorème permet de montrer qu'un groupe d'automorphismes d'un groupe polycyclique quelconque G est de présentation finie (L. Auslander, *Ann. Math.*, 1969, 89, n° 2, p. 314-322). En effet, si Hol $G \leqslant \mathbf{GL}_n(\mathbb{Z})$ et G est fermé en topologie polynomiale, son normalisateur et son centralisateur dans $\mathbf{GL}_n(\mathbb{Z})$ sont fermés eux aussi, donc sont de présentation finie (A. Borel, *Proc. Internat. Congress of Methns*, Stockholm, 1962, p. 10-22). Aussi le groupe Aut $G \simeq N_*(G)/C_*(G)$ est-il de présentation finie. Si G n'est pas fermé, le raisonnement devient un peu plus compliqué. Les détails et d'autres commentaires intéressants concernant le théorème 21.3.2 peuvent être trouvés dans le rapport de Wehrfritz au symposium de Londres du 22 juin 1973 [37].

A propos de la construction que nous avons indiquée en passant en fin de la démonstration du théorème 21.3.2, notons une

21.3.5. Question [36]. Soit C un groupe non trivial donné (par exemple $C = \mathbb{Z}_2$). On sait (*Alguebra i loguika*, 1970, 9, n° 5, p. 539-558) que pour deux groupes quelconques A, B toutes les extensions scindées de B par A se plongent d'une façon unique dans le produit direct $A \times \mathrm{Aut}\,(B \wr C)$. Comment y sont-elles disposées ?

§ 22. Généralisations de la résolubilité

22.1. Classes de Kouroch-Tchernikov. Nous disons que le groupe est résoluble s'il admet une matriochka sous-normale finie à sections abéliennes, ou une matriochka normale finie à sections abéliennes, ou encore si sa série dérivée devient stationnaire sur l'unité : toutes ces conditions sont équivalentes. Il serait intéressant d'étudier les matriochkas sous-normales infinies des différents types, de dégager les propriétés des classes obtenues et d'établir les liens entre elles (on s'attend naturellement à ce que les conditions énumérées cessent d'être équivalentes dans le cas général). Une telle théorie des « groupes résolubles généralisés » existe ; ses fondements ont été exposés dans le travail de A. G. Kouroch et S. N. Tchernikov [21]. Les classes de groupes résolubles généralisés, considérées dans le cadre de cette théorie seront appelées *classes de Kouroch-Tchernikov*, bien que certaines d'entre elles aient été étudiées encore avant le travail [21]. Nous conservons aussi les définitions et les désignations des classes de Kouroch-Tchernikov.

La notion fondamentale de la théorie des classes de Kouroch-Tchernikov est celle de la matriochka sous-normale, qui n'est pas nécessairement finie.

Un système $\mathcal{M}$ de sous-groupes du groupe G s'appelle *matriochka sous-normale* si G ;

1° il contient 1 et G;

2° il est totalement ordonné par inclusion, i.e. pour tous A, $B^{\#}$ de $\mathcal{M}$ on a soit $A \leqslant B$, soit $B \leqslant A$;

3° il est fermé par rapport à la réunion et l'intersection ; en particulier, avec tout $A \neq G$ il contient l'intersection $A^{\#}$ de tous les $H \in \mathcal{M}$ tels que $H > A$, et avec tout $B \neq 1$, la réunion $B^{\flat}$ de tous les $H \in \mathcal{M}$ tels que $H < B$;

4° il vérifie la condition $A \trianglelefteq A^{\#}$ pour tout $A \in \mathcal{M}$, $A \neq G$.

Les groupes quotients $A^{\#} A$ s'appellent *sections* de la matriochka sous-normale $\mathcal{M}$. On dit que $\mathcal{M}$ est *totalement ordonnée par croissance* si $A^{\#} \neq A$ pour tout $A \neq G$, et *totalement ordonnée par décroissance* si $B^{\flat} \neq B$ pour tout $B \neq 1$. Une matriochka sous-normale est dite *normale* si tous ses termes sont normaux dans le groupe. Si une matriochka sous-normale en contient une autre, on dit que la première est *plus fine* que la seconde, ou qu'elle est une *subdivision* de la seconde. En généralisant la définition donnée dans le n° 16.1, on

dit que la matriochka normale $\mathcal{M}$ est *centrale* si toutes ses sections sont centrales, i.e. si

$$A^{\#}/A \leqslant Z\,(G/A) \text{ pour tout } A \in \mathcal{M},\ A \neq G,$$

ou, ce qui revient au même, si

$$[A^{\#}, G] \leqslant A \text{ pour tout } A \in \mathcal{M},\ A \neq G.$$

Enfin, la matriochka sous-normale est appelée *résoluble* si ses sections sont toutes abéliennes.

On distingue les *classes de Kouroch-Tchernikov* suivantes (nous conservons les symboles traditionnels bien qu'ils ne soient pas très bien choisis à notre avis):

RN: le groupe admet une matriochka sous-normale résoluble (qui n'est pas nécessairement finie, ce qui sera toujours sous-entendu sans être dit explicitement);

RN^*: le groupe admet une matriochka sous-normale résoluble, totalement ordonnée par croissance;

$\overline{RN}$: toute matriochka sous-normale du groupe admet une matriochka sous-normale résoluble plus fine;

RI: le groupe admet une matriochka normale résoluble;

RI^*: le groupe admet une matriochka normale résoluble, totalement ordonnée par croissance;

$\overline{RI}$: toute matriochka normale du groupe admet une matriochka normale résoluble plus fine;

Z: le groupe admet une matriochka centrale;

ZA: le groupe admet une matriochka centrale, totalement ordonnée par croissance;

ZD: le groupe admet une matriochka centrale, totalement ordonnée par décroissance;

$\overline{Z}$: toute matriochka normale du groupe admet une matriochka centrale plus fine;

$\tilde{N}$: tout sous-groupe du groupe peut être inclus dans une matriochka sous-normale;

N: tout sous-groupe du groupe peut être inclus dans une matriochka sous-normale, totalement ordonnée par croissance.

Les matriochkas qui possèdent les propriétés indiquées s'appelleront respectivement: *RN-matriochka*, *RN^*-matriochka*, etc.

22.1.1. Exercice. La condition N est équivalente à la condition du normalisateur du n° 18.2.

22.1.2. Exercice. Pour les groupes finis, les conditions RN, RN^*, $\overline{RN}$, RI, RI^*, $\overline{RI}$ sont équivalentes à la résolubilité, et les conditions Z, ZA, ZD, $\overline{Z}$, $\tilde{N}$, N, à la nilpotence.

22.1.3. Exercice. Un groupe admet la propriété $\overline{RI}$ (resp. $\overline{Z}$) si et seulement si toutes ses images homomorphes admettent la propriété RI (resp. Z).

22.1.4. Exercice. Les propriétés RN^*, RI^*, ZA, $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\tilde{N}$, N restent valables pour les images homomorphes.

Plusieurs propriétés des groupes résolubles et nilpotents s'étendent sans peine (sans modifier la démonstration) aux généralisations de ces groupes:

22.1.5. Exercice. Le stabilisateur d'une matriochka normale quelconque admet une matriochka centrale. (Cf. le lemme 16.3.1.)

22.1.6. Exercice. Le commutant d'un groupe quelconque admettant une matriochka normale à sections cycliques admet une matriochka centrale. (Cf. le théorème 19.2.2.)

22.1.7. Exercice. Tout sous-groupe normal abélien maximal A d'un ZA-groupe G se confond avec son centralisateur. En particulier, A est un sous-groupe abélien maximal et G/A admet une image isomorphe dans Aut A. (Cf. le théorème 16.2.6.)

Les classes de Kouroch-Tchernikov sont vastes: par exemple, la classe Z contient, en vertu du théorème de Magnus 14.4.4, tous les groupes libres. Un fait moins évident: tout groupe libre dénombrable admet une image isomorphe dans un groupe appartenant à la classe $\overline{Z}$. Nous le montrerons à l'aide d'un exemple.

22.2. Exemples. Un exemple important des groupes résolubles généralisés est fourni par les groupes ordonnables.

22.2.1. Exemple. Tout groupe ordonnable G possède la propriété RN (rappelons qu'un groupe est dit *ordonnable* s'il peut être muni de la relation d'ordre total $\leqslant$ stable pour la multiplication; pour plus de détails, voir le n° 27.2 de l'Appendice). Soit en effet G un groupe muni de la relation d'ordre total $\leqslant$. Sa partie V est dite *convexe* si, avec ses deux éléments quelconques a, b, elle contient aussi tous les éléments intermédiaires, i.e. si

$$a \in V, \quad b \in V, \quad a \leqslant x \leqslant b \Rightarrow x \in V.$$

Il se trouve que le système $\mathscr{M}$ de tous les sous-groupes convexes d'un groupe ordonné G est une matriochka sous-normale résoluble. En effet, la condition 1° figurant dans la définition d'une matriochka sous-normale est évidente. Vérifions la condition 2°. Soient A, B deux sous-groupes convexes, et soit un élément $b \in B$, $b \notin A$, par exemple $b > 1$. Il est clair que $a \leqslant b$ pour tout $a \in A$. Puisque $1 \leqslant a \leqslant b$ ou $1 \leqslant a^{-1} \leqslant b$, on a $A \leqslant B$, comme demandé. La condition 3° est immédiate. Vérifions la condition 4° selon laquelle $A \lhd B$, où A, B sont deux sous-groupes convexes tels que $A < B$;

il n'y a aucun autre sous-groupe convexe entre A et B. Pour tout $b \in B$, on a $A^b < B^b$; il est clair d'ailleurs que A^b, B^b sont encore des sous-groupes convexes et qu'il n'existe aucun autre sous-groupe convexe entre eux. Puisque $B^b = B$, on a $A^b = A$, ce qu'il fallait démontrer. Enfin, chaque section $A^{\#}/A$ de la matriochka $\mathcal{M}$ est un groupe ordonné sans aucun sous-groupe propre convexe. En vertu du théorème classique de Hölder sur les groupes ordonnés (sa démonstration, citée dans [18], n'occupe pas une page, étant entièrement basée sur les définitions), la section $A^{\#}/A$ admet une image isomorphe dans le groupe additif du corps $\mathbb{R}$; en particulier, cette section est un groupe abélien, d'où il découle que $\mathcal{M}$ est une matriochka sous-normale résoluble.

Examinons maintenant les exemples de groupes nilpotents généralisés. Il est intéressant de considérer à ce titre les différents groupes de congruence, que ce soient les groupes classiques $\Gamma_n(m)$ sur l'anneau $\mathbb{Z}$ ou les groupes analogues sur d'autres anneaux. Commençons par un

22.2.2. Exemple (Iou. I. Merzliakov in: *Alguebra i loguika*, 1963, 2, n° 5, p. 29-36). Soit k un ensemble contenant le zéro et tous les nombres rationnels qui gardent après simplifications un dénominateur impair. Il est évident que k est un anneau. Soit

$$G_n = \begin{pmatrix} 1+2^n k & 2^n k \\ 2^n k & 1+2^n k \end{pmatrix}, \quad n = 1, 2, \ldots,$$

i.e. G_n est un ensemble de matrices dont les éléments parcourent, indépendamment les uns des autres, les ensembles correspondants de nombres rationnels. On voit sans peine que chaque G_n est un groupe. Nous savons que le groupe G_1 contient un sous-groupe libre de rang 2 (voir le théorème 14.2.1), donc aussi des sous-groupes libres de tout rang fini ou dénombrable. Montrons que G_1 admet également la propriété $\overline{Z}$, i.e. que le groupe quotient de G_1 par tout sous-groupe normal H admet une matriochka centrale (voir l'exercice 22.1.3).

Tout d'abord, si H est inclus dans le centre de G_1, le système de groupes quotients

$$G_1/H \geqslant G_2H/H \geqslant \ldots \geqslant \bigcap_{n=1}^{\infty} (G_nH/H) \geqslant 1$$

est visiblement une matriochka centrale du groupe quotient G_1/H. Supposons maintenant que le sous-groupe normal H n'est pas contenu dans le centre de G_1 et montrons qu'on a alors

$$H \geqslant T \cap G_n \text{ pour un certain } n, \tag{1}$$

où T est l'ensemble des matrices de déterminant 1 dans G_1. Cela aura achevé la démonstration, car G_1/H sera alors une image homo-

morphe du groupe $G_1/T \cap G_n$ qui, en vertu du théorème de Remak 4.3.9, se plonge dans le produit direct du groupe abélien G_1/T et du groupe nilpotent G_1/G_n. Quant à la proposition (1), elle sera démontrée en utilisant de nouveau la méthode philosophique fructueuse d'extraction de la chaîne (voir page 104):

a) Le sous-groupe H contient une matrice h telle que $h_{11}^2 \neq h_{22}^2$. En effet, soit c une matrice non scalaire quelconque de H. On vérifie immédiatement qu'il est possible de choisir comme h n'importe laquelle des matrices c, c^a, c^b, $c^a c$, $c^b c$, $c^a c^b$, où $a = t_{12}(2)$, $b = t_{21}(2)$.

b) Si H contient h, il contient alors également les transvections $t_{12}(\lambda)$, $t_{21}(\lambda)$, où $\lambda = 2\mu((h_{22}^2/h_{11}^2) - 1)$, μ un nombre rationnel quelconque de numérateur et dénominateur impairs. En effet, on vérifie immédiatement que $t_{12}(\lambda) = [a, h^u h]^v$, où $a = t_{12}(2)$, $u = \operatorname{diag}(-h_{22}, h_{11})$, $v = \operatorname{diag}(1, \mu)$. Quant à la matrice $t_{21}(\lambda)$, elle s'obtient par la transposition de cette relation; remarquons que h peut être laissée sans transposition, vu que λ ne dépend que de ses éléments diagonaux. Etablissons une formule fort utile pour ces calculs:

$$x^d = \begin{pmatrix} x_{11} & \frac{\beta}{\alpha} x_{12} \\ \frac{\alpha}{\beta} x_{21} & x_{22} \end{pmatrix} \quad \text{pour } d = \operatorname{diag}(\alpha, \beta).$$

c) Il existe un $m \geqslant 1$ tel que H contient toutes les transvections $t_{12}(2^m \varkappa)$, $t_{21}(2^m \varkappa)$, $\varkappa \in k$: cela ressort immédiatement de a) et b).

d) Le sous-groupe H contient une matrice arbitraire

$$x = \begin{pmatrix} 1 + 2^{2m}\alpha & 2^{2m}\beta \\ 2^{2m}\gamma & 1 + 2^{2m}\delta \end{pmatrix}, \quad \alpha, \beta, \gamma, \delta \in k, \quad \det x = 1.$$

En effet, il est facile de voir que

$$x = t_{12}(2^m \xi)\, t_{21}(2^m \delta)\, t_{12}(2^m)\, t_{21}(2^m \eta), \tag{2}$$

où

$$\xi = \frac{2^m \beta - 1}{x_{22}}, \qquad \eta = \frac{2^m \gamma - \delta}{x_{22}}.$$

L'extraction des maillons est terminée.

En passant, nous avons apporté une réponse positive au problème de congruence pour $\mathrm{SL}_2(k)$. En effet, soit H un sous-groupe normal d'indice fini n dans $\mathrm{SL}_2(k)$. Puisque les n-ièmes puissances des transvections de $\mathrm{SL}_2(k)$ sont contenues dans H, la condition c) est vérifiée. Comme c) $\Rightarrow$ d), H est un sous-groupe de congruence.

Remarquons que le 2 n'a joué aucun rôle essentiel dans le raisonnement. On établit d'une façon analogue, par exemple, le résultat

suivant. Soit π l'ensemble obtenu en éliminant une partie finie (nous la noterons π') dans l'ensemble de tous les nombres premiers. Soit $\mathbb{Q}_\pi$ l'anneau des fractions π-aires, i.e. des nombres rationnels dont les dénominateurs sont divisibles par des seuls nombres premiers appartenant à π. Chaque sous-groupe H d'indice fini n dans $\mathrm{SL}_2(\mathbb{Q}_\pi)$ est un sous-groupe de congruence. En effet, soient H un sous-groupe normal et q le produit de tous les nombres de π'. Choisissons un majorant $m \geqslant 1$ des exposants avec lesquels les diviseurs appartenant à π' interviennent dans n. Puisque H contient toutes les transvections $t_{ij}(q^m\varkappa)$, $\varkappa \in \mathbb{Q}_\pi$, notre proposition résulte de la décomposition suivante analogue à (2) pour $\mu = \mu' = q^m$:

$$x \equiv \begin{pmatrix} 1+\mu\mu'\alpha & \mu\mu'\beta \\ \mu\mu'\gamma & 1+\mu\mu'\delta \end{pmatrix} = t_{12}(\mu\xi)\, t_{21}(\mu'\delta)\, t_{12}(\mu)\, t_{21}(\mu'\eta). \qquad (2')$$

où

$$\det x = 1, \quad \xi = \frac{\mu'\beta - 1}{x_{22}}, \qquad \eta = \frac{\mu\gamma - \delta}{x_{22}}.$$

De l'exemple 22.2.2 on voit que les propriétés $\overline{RI}$ et $\overline{Z}$ ne s'étendent pas aux sous-groupes, car les groupes libres non cycliques n'ont pas ces propriétés (voir l'exercice 22.1.4).

Poursuivant le travail exposé, G.A. Noskov a montré (*Sib. matem. j.*, 1973, 14, n° 3, p. 680-683) que le groupe G_1 admet aussi la propriété $\overline{RN}$, si bien que cette dernière ne s'étend pas aux sous-groupes, elle non plus.

Pour les groupes topologiques, les conditions de finitude et de résolubilité généralisée ont été étudiées par V.M. Glouchkov, V.S. Tcharine et d'autres.

22.3. Théorème local. Un système M_i, $i \in I$, de parties d'un ensemble M s'appelle *recouvrement local* de M si tout élément de M est contenu dans un M_i et deux ensembles quelconques M_i, M_j sont contenus dans un troisième ensemble M_k. Comme exemples de recouvrements locaux, citons l'ensemble des parties finies d'un ensemble donné et l'ensemble des sous-groupes de type fini d'un groupe donné. On dit que *le groupe G admet localement une propriété* σ s'il existe un recouvrement local de G constitué de sous-groupes qui admettent σ. Il est clair que pour une propriété σ applicable aux sous-groupes, le groupe G admet localement σ si et seulement si chaque sous-groupe de type fini dans G admet σ. Les exemples des propriétés locales sont fournis par la nilpotence locale et la finitude locale que nous avons examinées dans le chapitre précédent.

On dit qu'une propriété des groupes (et de la classe correspondante des groupes) vérifie le *théorème local* si chaque groupe admettant localement la propriété en question admet cette dernière lui-même.

Par exemple, le théorème local a lieu dans la classe des groupes abéliens et n'a pas lieu dans celle des groupes finis.

Pourquoi le théorème local est-il vérifié pour certaines propriétés et ne l'est pas pour d'autres ? En se posant cette question, A.I. Maltsev a remarqué (*Outch. zap. Ivanovskogo ped. in-ta*, 1941, 1, n° 1, p. 3-9) que les théorèmes locaux ne sont pas particuliers à la théorie des groupes mais sont tout aussi naturels pour les anneaux, les boucles et d'autres structures algébriques et que, par conséquent, leur raison d'être ne réside pas dans la théorie des groupes ou dans une autre théorie particulière mais dans les fondements des mathématiques. Cette remarque s'est avérée très juste : tout un bouquet de théorèmes locaux a son fondement conceptuel dans un résultat connu de la logique formelle selon lequel tout théorème issu d'un certain nombre d'axiomes se laisse déduire d'une partie finie de ce nombre d'axiomes. En développant cette remarque, A.I. Maltsev a abouti à son théorème de compacité du calcul des prédicats restreint, et ensuite, au théorème local pour une propriété quelconque écrite au moyen de formules dites quasi universelles. La question d'applicabilité du théorème local à une propriété donnée σ, qui était traitée séparément pour chaque σ avant les travaux de A.I. Maltsev, s'est trouvée réduite, grâce à ses travaux, à une question générale et purement « grammaticale » : est-il possible d'écrire σ au moyen d'axiomes quasi universels ?

A l'aide d'un artifice ingénieux que nous décrirons, A.I. Maltsev, déjà dans son travail datant de 1941, a écrit les propriétés RN, RI, Z avec des formules quasi universelles d'un type particulier et a montré, par ce procédé, qu'elles vérifient le théorème local. Plus tard, il est revenu à sa méthode pour lui donner sa généralité d'aujourd'hui et, dans son travail *Correspondances modèles* (*Izv. AN SSSR*, sér. math., 1959, **23**, n° 3, p. 313-336), il a déduit d'une façon uniforme pratiquement tous les théorèmes locaux intéressants de la théorie des groupes. On peut dire que si le travail de 1941 jetait un premier pont entre les théorèmes locaux de l'algèbre et la logique, le travail de 1959 a réduit ce pont aux dimensions d'un trait d'union. Par ailleurs, le premier travail allait servir de point de départ à la théorie des modèles.

Utilisant la méthode de A.I. Maltsev, nous démontrerons ici le théorème local pour les classes de Kouroch-Tchernikov. Un exposé « clos » de la partie logique de la méthode est donné au § 27 de l'Appendice. Si le lecteur n'est pas au courant de cette méthode, il doit se reporter à présent à l'Appendice avant de continuer la lecture.

22.3.1. Théorème (A.I. Maltsev). *Les propriétés RN, RI, Z, $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\tilde{N}$ vérifient le théorème local.*

Démonstration. Utilisant l'artifice proposé par A.I. Maltsev (voir ci-dessus), passons du langage des matriochkas sous-norma-

les à celui des prédicats. A cet effet, à chaque matriochka sous-normale $\mathscr{M}$ des sous-groupes du groupe G, associons un prédicat P sur G en posant $P(x, y) = \mathrm{V}$ (= vrai) si et seulement si dans $\mathscr{M}$ il existe un sous-groupe contenant x mais ne contenant pas y. Il est clair que P vérifie les axiomes universels suivants (écrits sans quantificateurs) :

1° $\neg P(x, x)$,
2° $P(x, y) \wedge P(y, z) \to P(x, z)$,
3° $P(x, z) \wedge \neg P(y, z) \to P(x, y)$,
4° $P(x, z) \wedge P(y, z) \to P(xy^{-1}, z)$,
5° $x \neq 1 \to P(1, x)$,
6° $P(x, y) \to P(y^{-1}xy, y)$.

Introduisons la notation $A_y = \{x \mid x \in G, P(x, y) = \mathrm{V}\}$, $y \neq 1$. On voit sans peine que

$$A_y = \bigcup_{y \notin A \in \mathscr{M}} A, \quad A = \bigcap_{y \notin A} A_y \quad (A \in \mathscr{M},\ A \neq G)$$

i.e. que $A_y \in \mathscr{M}$ et que chaque $A \in \mathscr{M}$, $A \neq G$, se laisse mettre sous forme d'intersection de sous-groupes A_y.

Réciproquement, soit défini sur G un prédicat P vérifiant les propriétés 1° à 6°. Les ensembles A_y forment une famille de sous-groupes totalement ordonnée par inclusion. En ajoutant à cette famille le groupe G, ainsi que les réunions et les intersections de toutes les sous-familles, nous obtenons une matriochka sous-normale de sous-groupes dans le groupe G. Des axiomes 1° à 3° il ressort immédiatement que les transitions indiquées de $\mathscr{M}$ à P et de P à $\mathscr{M}$ sont inverses entre elles, ce qui confirme qu'elles assurent la traduction cherchée dans le langage CP.

Traduites dans le langage CP, les notions fondamentales de la théorie des classes de Kouroch-Tchernikov se présentent comme suit :

7° la matriochka est résoluble : $x \neq 1 \wedge \neg P(x, y) \wedge \wedge \neg P(y, x) \to P([x, y], x)$,

8° la matriochka est normale : $P(x, y) \to P(z^{-1}xz, y)$,

9° la matriochka est centrale : $x \neq 1 \to P([x, y], x)$.

Caractérisons encore les matriochkas à trois termes $1 \leqslant A \leqslant G$ dans le langage CP. Pour le faire, on doit évidemment ajouter aux axiomes 1° à 5° l'axiome

10° la matriochka est à trois termes : $x \neq 1 \wedge P(x, y) \to \to \neg P(y, z)$.

Il est clair maintenant que les propriétés RN, RI, Z se définissent par les formules

RN : $(\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge 7))$,
RI : $(\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (7) \wedge (8))$,
Z : $(\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (9))$,

où (1), (2), . . . sont des expressions de 1°, 2°, . . ., tandis que les

propriétés $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\tilde{N}$ traduisant la possibilité de la subdivision s'écrivent au moyen des formules

$$\overline{RN}: \ (\forall P)\,((P = \text{sous-norm.}) \to (\exists Q)\,((Q = \text{résol. sous-norm.}) \wedge \wedge (\forall u)\,(\forall v)\,(P\,(u, v) \to Q\,(u, v)))),$$

$$\overline{RI}: \ (\forall P)\,((P = \text{norm.}) \to (\exists Q)\,((Q = \text{résol. norm.}) \wedge (\forall u)\,(\forall v)\,(P\,(u, v) \to Q\,(u, v)))),$$

$$\overline{Z}: \ (\forall P)\,((P = \text{norm.}) \to (\exists Q)((Q = \text{centr.}) \wedge (\forall u)(\forall v)\,(P\,(u, v) \to Q\,(u, v)))),$$

$$\tilde{N}: \ (\forall P)\,((P = \text{à 3 termes}) \to (\exists Q)\,((Q = \text{sous-norm.}) \wedge (\forall u)\,(\forall v)\,(P\,(u, v) \to Q\,(u, v)))),$$

dans lesquelles les abréviations sont à remplacer par des combinaisons évidentes des formules 1° à 10°. Puisque toutes les sept propriétés se sont avérées quasi universelles, il ne reste qu'à faire intervenir le théorème 27.3.3 de l'Appendice. Le théorème est démontré.

Les propriétés RN^*, RI^*, ZA, ZD, N non couvertes par le théorème de Maltsev ne vérifient pas le théorème local (voir en particulier l'exemple 18.2.2).

Rappelons que les formules pour RN, RI, Z sont objet-universelles, aussi les propriétés indiquées s'étendent-elles aux sous-groupes en vertu du théorème 27.3.1 de l'Appendice (ce fait est d'ailleurs facile à démontrer immédiatement).

22.3.2. Exercice. Les propriétés RN^*, RI^*, ZA, ZD, N, $\tilde{N}$ s'étendent aux sous-groupes, elles aussi.

CHAPITRE 8

CONDITIONS DE FINITUDE

§ 23. La périodicité et la finitude locale

23.1. Ces deux notions coïncident-elles ? Rappelons qu'un groupe est dit *périodique* si chacun de ses éléments est d'ordre fini. Un groupe est dit *localement fini* si tous ses sous-groupes de type fini sont finis. Il est clair que tout groupe localement fini est périodique. La réciproque est-elle vraie ? Cette question constitue le problème de Burnside qui date du début de ce siècle. Plus exactement, il se présente en trois variantes :

I. Problème de Burnside général $\mathfrak{B}$: tout groupe périodique est-il localement fini ?

II. Problème de Burnside restreint $\mathfrak{B}(r, m)$: tout groupe de période donnée m, i.e. vérifiant identiquement $x^m = 1$, ayant un nombre donné r de générateurs, est-il fini ?

III. Problème de Burnside affaibli $\mathfrak{B}'(r, m)$: le nombre des groupes f i n i s de période donnée m, ayant un nombre donné r de générateurs, est-il fini ?

Il est clair que la réponse négative de $\mathfrak{B}(r, m)$ pour r, m quelconques entraîne la réponse négative de $\mathfrak{B}$ et que la réponse positive de $\mathfrak{B}(r, m)$ entraîne la réponse positive de $\mathfrak{B}'(r, m)$.

Voici l'état de nos connaissances à l'heure actuelle en ce qui concerne ces trois questions :

I. E.S. Golod (*Izv. AN SSSR*, série math., 1964, **28**, n° 2, p. 273-276) et S.V. Aliochine (*Matem. zametki*, 1972, **11**, n° 3, p. 319-328) ont construit des exemples de groupes périodiques infinis de type fini, ce qui donne la réponse négative au problème de Burnside général. Il va sans dire qu'une solution à ce problème est donnée, en passant, par l'exemple récent de A. Iou. Olchanski que nous avons mentionné au § 2 à l'occasion du problème de O. Iou. Schmidt.

II. P.S. Novikov et S.I. Adian (*Izv. AN SSSR*, série math., 1968, **32**, p. 212-244, 251-524, 709-731) ont démontré l'infinitude du groupe libre $\mathbf{B}_r(m)$ dans la variété des groupes vérifiant identiquement $x^m = 1$, à r générateurs libres, avec $r \geqslant 2$ et m impair $\geqslant 4381$. Ce majorant a été abaissé plus tard jusqu'à $m \geqslant 665$, cf. [1]. D'autre part, on connaît quelques groupes libres de Burnside de faible période

qui sont finis: $B_r(2)$ (exercice), B_r (3) (Burnside, 1902), B_r (4) (I.N. Sanov, 1940) et B_r (6) (M. Hall, 1957). Il manque sur cette liste le groupe B_r (5) dont on ignore toujours s'il est fini ou non.

III. A.I. Kostrikine (*Izv. AN SSSR*, série math., 1959, **23**, n° 1, p. 3-34; voir aussi in *Matem. sb.*, 1979, **110**, n° 1, p. 3-12) a donné la réponse positive au problème de Burnside affaibli $\mathfrak{B}'$ (r, m) pour m premier.

Ainsi donc, le problème de Burnside général est résolu; néanmoins on ne connaît actuellement que quelques groupes périodiques isolés qui ne sont pas localement finis, ou, mieux, quelques types constructifs de tels groupes. Il est difficile de dire s'il y en aura d'autres, mais aujourd'hui ces rares exemples nous font autant d'effet que les échantillons du sol lunaire. Chacun d'eux mérite sans conteste une attention minutieuse, à tel point que nous consacrons tout un paragraphe à la remarquable construction de S.V. Aliochine. (L'exemple dû à E.S. Golod a été décrit plus haut, voir l'exemple 18.3.2; voir aussi le § 26 de l'Appendice. Quant aux autres constructions mentionnées, elles sont malheureusement trop encombrantes pour trouver leur place dans un ouvrage d'enseignement.)

A propos, remarquons qu'à la différence du cas général, le problème de Burnside relatif aux groupes linéaires a été résolu, positivement, encore au début du siècle, voir [25], p. 409.

Pour terminer cette série de remarques préliminaires, citons une propriété importante des groupes localement finis (qui s'étend d'ailleurs sans difficulté aucune aux groupes périodiques):

23.1.1. Théorème (O. Iou. Schmidt). *L'extension G d'un groupe localement fini A par le groupe localement fini G/A est elle-même un groupe localement fini.*

Démonstration. Vérifions que tout ensemble fini M dans G engendre un sous-groupe fini. Par hypothèse, le groupe quotient gr $(M, A)/A$ est fini. En prenant au besoin un ensemble M plus grand, supposons que M soit fermé pour l'inversion et contienne les représentants de toutes les classes de gr (M, A) suivant A. Pour tous x, y de M on a alors

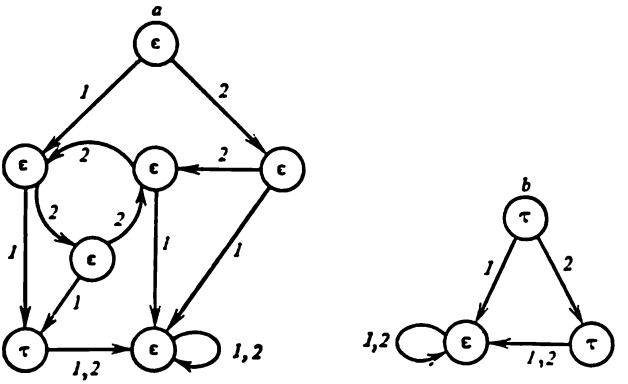
$$xy = \overline{xy} \cdot a_{x,y}, \quad \text{où } \overline{xy} \in M, \quad a_{x,y} \in A.$$

Il s'ensuit que tout produit d'éléments de M se laisse mettre sous la forme de produit d'un élément de M par le produit de certains $a_{x,y}$. Puisque tous les $a_{x,y}$ engendrent un sous-groupe fini, le théorème est démontré.

23.2. Le 2-groupe infini 2-engendré des transformations séquentielles. Dans son exemple mentionné plus haut, S.V. Aliochine a construit un p-groupe infini 2-engendré de transformations séquentiel-

les, i.e. réalisées sur les automates, qui admet une approximation finie, pour tout p premier. L'idée de la construction ressort clairement déjà dans le cas le plus simple où $p = 2$; nous nous bornerons donc à considérer ce cas.

Qu'est-ce qu'un automate et comment travaille-t-il? Sans exposer ici la théorie générale des automates, nous nous contentons d'examiner les schémas de deux automates a, b dont nous aurons besoin:



Par définition, ces automates opèrent sur l'ensemble K_2^ω de toutes les séquences (i.e. suites finies) de chiffres 1, 2. L'automate a admet sept états représentés sur son schéma par des cercles; le premier état — l'état initial — est marqué de la lettre a. Dans les cercles, viennent s'inscrire les permutations de l'ensemble $I = \{1, 2\}$: ε est la permutation identique et τ la transposition. L'automate travaille comme suit. Soit une séquence $\gamma = i_1 i_2 \ldots i_m$. L'automate répond au premier terme i_1 de la séquence par la permutation ε correspondant à son état initial et passe dans un nouvel état suivant la flèche i_1, puis répond à i_2 par la permutation correspondant à ce nouvel état et sort de cet état suivant la flèche i_2, et ainsi de suite. Il est commode d'introduire une notation spéciale: si, après avoir traité la séquence γ, l'automate a passe à l'état figuré par la permutation π, nous écrirons

$$a/\gamma \sim \pi.$$

Soit par exemple $\gamma = 121221$. En suivant les flèches de l'automate a à la manière du jeu de l'oie, nous constatons que

$$a/1 \sim \varepsilon,$$
$$a/12 \sim \varepsilon,$$
$$a/121 \sim \tau,$$
$$a/1212 \sim \varepsilon,$$

$$a/12122 \sim \varepsilon,$$
$$a/121221 \sim \varepsilon,$$

donc $\gamma a = 1^{\varepsilon}2^{\varepsilon}1^{\varepsilon}2^{\tau}2^{\varepsilon}1^{\varepsilon} = 121121$ et $a/\gamma \sim \varepsilon$.

L'automate b travaille d'une façon analogue.

23.2.1. Exercice. Dans toute séquence, l'automate a change un chiffre tout au plus; le segment antérieur à ce chiffre se présente sous la forme $i2\ldots21$. En faisant travailler a une fois de plus, nous retrouvons la séquence initiale, quelle qu'elle ait été, si bien que $a^2 = 1$ (le lecteur remarquera que nous identifions l'automate et la transformation qu'il produit sur l'ensemble des séquences K_2^{ω}). En particulier, a est une transformation biunivoque inverse d'elle-même. Voici la liste complète des cas où l'automate a passe à l'état (unique) correspondant à la permutation τ: si long. $\gamma \geqslant 3$, on a $a/\gamma \sim \tau$ si et seulement si

$$\gamma = \begin{cases} 12\ldots21 & \text{pour long. } \gamma \equiv 0 \pmod 3, \\ 22\ldots21 & \text{pour long. } \gamma \equiv 1 \pmod 3, \\ i2\ldots21 & \text{pour long. } \gamma \equiv 2 \pmod 3. \end{cases}$$

23.2.2. Exercice. L'automate b travaille tout simplement:

$$\begin{tikzcd} 11\eta \arrow[r, "b"] & 21\eta \arrow[d, "b"] \\ 22\eta \arrow[u, "b"] & 12\eta, \arrow[l, "b"] \end{tikzcd}$$

où η est une séquence quelconque. En particulier, b ne change que les deux premiers termes de la séquence, de telle façon que tout couple de termes se laisse déduire de tout autre couple en faisant agir b autant de fois que nécessaire. Ensuite, $b^4 = 1$, si bien que b est aussi une transformation biunivoque de l'ensemble K_2^{ω} (avec la transformation inverse b^3).

23.2.3. Théorème (S.V. Aliochine). *Le groupe des transformations séquentielles $G = \mathrm{gr}\,(a, b)$ est un 2-groupe infini qui se laisse approcher par des 2-groupes finis.*

Démonstration. a) Le groupe G est infini. En effet, il suffit de trouver dans G des éléments $x_1, x_2, \ldots$ tels que

$$\underbrace{1\ldots1}_{k-1}2\eta \xrightarrow{x_k} \underbrace{1\ldots1}_{k}\eta$$

pour toute séquence η, car, en prenant $y_k = x_1 \ldots x_k$, on obtient

$$\underbrace{2\ldots22}_{k}\ldots \xrightarrow{y_k} \underbrace{1\ldots12}_{k}\ldots,$$

i.e. il existe dans G une infinité d'éléments distincts $y_1, y_2, \ldots$

Il est clair qu'on peut prendre $x_1 = b^3$, $x_2 = b^2$ (voir l'exercice 23.2.2). Supposons maintenant que les éléments $x_1, \ldots, x_{k-1}$, $k \geqslant 3$, soient déjà construits, et construisons x_k. Il vient

$$\underbrace{1\ldots12}_{k-1}\eta \xrightarrow{x_{k-2}^{-1}} \underbrace{1\ldots1212}_{k-3}\eta \xrightarrow{x_{k-3}^{-1}} \ldots \xrightarrow{x_1^{-1}} \underbrace{2\ldots212}_{k-2}\eta. \qquad (1)$$

De la définition de l'automate a on voit (voir aussi l'exercice 23.2.1) que

$$\underbrace{12\ldots212}_{m}\eta \xrightarrow{a} \underbrace{12\ldots211}_{m}\eta \quad \text{pour } m \equiv 0, \text{ ou } 1 \pmod 3,$$

$$\underbrace{22\ldots212}_{m}\eta \xrightarrow{a} \underbrace{22\ldots211}_{m}\eta \quad \text{pour } m \equiv 2 \pmod 3.$$

Il suffit donc de changer si nécessaire dans la dernière séquence de la chaîne (1) le premier chiffre (à l'aide d'une puissance convenable de la transformation b), d'appliquer ensuite a et peut-être encore une puissance convenable — inverse — de b pour obtenir

$$\underbrace{2\ldots211}_{k-2}\eta.$$

Appliquant enfin $x_1 \ldots x_{k-2}$, on obtient la séquence cherchée $\underbrace{1\ldots1}_{k}\eta$. On peut donc prendre

$$x_k = x_{k-2}^{-1} \ldots x_1^{-1} b^{-m} a b^m x_1 \ldots x_{k-2}$$

en choisissant convenablement $m = 0$ ou 1.

b) Le groupe G se laisse approcher par des 2-groupes finis. Soient en effet I^n l'ensemble des séquences de longueur n de l'alphabet $I = \{1, 2\}$ et G_n le groupe des permutations de I^n induites (par restriction à I^n) par les transformations de G, $n = 1, 2, \ldots$ Il est clair que l'intersection des noyaux de tous les homomorphismes restrictions $G \to G_n$ est triviale ; il suffit donc de s'assurer que chaque G_n est un 2-groupe. A cet effet, nous montrerons par récurrence sur n que G_n est de période 2^n.

Soit d'abord $n = 1$. Tout élément $g \in G$ se laisse mettre sous la forme $g = b^{\beta_1} a b^{\beta_2} a \ldots b^{\beta_s}$ et opère sur un chiffre $i \in \{1, 2\}$, comme

la permutation $\tau^{\beta_1+\cdots+\beta_s}$. Il est clair que $ig^2 = i$. Supposons démontré que $\gamma g^{2^{n-1}} = \gamma$ pour tout $\gamma \in I^{n-1}$; soit $j \in \{1, 2\}$. Il est évident que $(\gamma j)\, g^{2^{n-1}} = \gamma j^{\tau^m}$, où $m = 0$ ou 1. Appliquant encore une fois la transformation $g^{2^{n-1}}$, on obtient $(\gamma j)\, g^{2^n} = \gamma j$.

c) Il ne reste qu'à montrer — mais c'est le plus difficile — que G est un 2-groupe. En vertu de b) le groupe G ne peut avoir aucune torsion autre que la 2-torsion; il suffit donc de montrer que G est périodique. Introduisons quelques notions auxiliaires en commençant par celle de la flexibilité d'une séquence dans une transformation séquentielle.

Soit γ une séquence de l'alphabet $\{1, 2\}$, et soit g un élément de G écrit d'une façon donnée à l'aide des générateurs

$$g = z_1 \ldots z_s, \text{ où chaque } z_k = a \text{ ou } b.$$

Soit ensuite d le plus petit entier naturel tel que $\gamma g^d = \gamma$. Ecrivons sous forme d'un tableau la suite $\Gamma_g(\gamma)$ de tous les résultats intermédiaires de l'application du mot $(z_1 \ldots z_s)^d$ à la séquence γ

$$\begin{array}{c|c|c|c|c}
 & z_1 & z_2 & z_{s-1} & z_s \\
\gamma = \gamma_1^1 & \gamma_2^1 & & & \gamma_s^1 \\
\gamma_1^2 & \gamma_2^2 & & & \gamma_s^2 \\
\vdots & \vdots & \cdots & & \vdots \\
\gamma_1^d & \gamma_2^d & & & \gamma_s^d
\end{array}$$

On a donc

$$\gamma_{k+1}^l = \gamma_k^l z_k \text{ pour } 1 \leqslant k \leqslant s-1, \quad 1 \leqslant l \leqslant d,$$
$$\gamma_1^{l+1} = \gamma_s^l z_s \text{ pour } 1 \leqslant l \leqslant d-1,$$

tandis que la suite $\Gamma_g(\gamma)$ elle-même s'obtient en lisant le tableau ligne après ligne. Soit ensuite $\tilde{\Gamma}_g(\gamma)$ la suite extraite de $\Gamma_g(\gamma)$, composée de toutes les γ_k^l de la forme $i2 \ldots 2j$ attaquées par $z_k = a$ (rappelons que les séquences de ce type sont les seules qui puissent faire changer le chiffre suivant à l'automate a, voir l'exercice 23.2.1). Si Γ est une suite finie, supposons que Γ° désigne la suite circulaire qu'on obtient à partir de Γ en écrivant son dernier terme avant le premier. Soit enfin $\mathrm{sgm}_g(\gamma)$ (resp. $\mathrm{sgm}_g^\circ(\gamma)$) le nombre des « 2-segments » connexes de la forme

$$i'2 \ldots 22, \ldots, i''2 \ldots 22$$

qui alternent dans la suite $\tilde{\Gamma}_g(\gamma)$ (resp. dans la suite circulaire $\tilde{\Gamma}_g^\circ(\gamma)$) avec les « 1-segments » connexes de la forme

$$i'2 \ldots 21, \ldots, i''2 \ldots 21$$

(on conçoit que si l'on a des segments des deux types, le nombre des uns et des autres dans $\widetilde{\Gamma}_g^\circ(\gamma)$ est le même, tandis que dans $\widetilde{\Gamma}_g(\gamma)$ le nombre des segments d'un type ne peut différer de celui des autres que d'une unité tout au plus). Nous disons que la quantité

$$\mathrm{fl}_g(\gamma) = \left[\frac{1}{2}\,\mathrm{sgm}_g^\circ(\gamma)\right]$$

est la *flexibilité* de la séquence γ dans la transformation g (plus exactement, dans l'écriture donnée de l'élément g par l'intermédiaire des générateurs a, b). Par exemple, si la partie « caudale » des séquences de $\widetilde{\Gamma}_g(\gamma)$ est de la forme 2122122112, on a $\mathrm{sgm}_g(\gamma) = 4$, $\mathrm{sgm}_g^\circ(\gamma) = 3$, $\mathrm{fl}_g(\gamma) = 1$. Informellement parlant, la flexibilité de la séquence traduit le nombre des remuements de la queue dans la suite $\widetilde{\Gamma}_g^\circ(\gamma)$.

23.2.4. Exercice. Si $\gamma g = \delta$, on a $\mathrm{sgm}_g^\circ(\gamma) = \mathrm{sgm}_g^\circ(\delta)$ et $\mathrm{fl}_g(\gamma) = \mathrm{fl}_g(\delta)$.

Remarquons que nous avons passé de sgm à sgm° rien que pour avoir cette propriété. Quant au partage en deux moitiés et au passage à la partie entière, leur seul but était de démontrer la proposition suivante.

d) Montrons que la flexibilité d'une séquence est en général d'autant moins grande que la séquence est plus longue. Plus exactement, pour tout $g \in G$, toute séquence γ de longueur $\geqslant 3$ et tout chiffre $j \in \{1, 2\}$ on a l'inégalité

$$\mathrm{fl}_g(\gamma j) \leqslant \mathrm{fl}_g(\gamma). \tag{2}$$

Il y a plus : si $\mathrm{fl}_g(\gamma) > 0$, d est le plus petit nombre tel que $\gamma g^d = \gamma$ et l'automate g^d passe sous l'action de γ à l'état correspondant à la permutation identique, i.e. $g^d/\gamma \sim \varepsilon$, alors

$$\mathrm{fl}_g(\gamma j) < \mathrm{fl}_g(\gamma). \tag{3}$$

Remarquons d'abord que si $i'2\ldots2$, $i''2\ldots2$ sont deux séquences voisines dans la suite $\widetilde{\Gamma}_g^\circ(\gamma)$, elles seront affectées d'un même chiffre dans $\widetilde{\Gamma}_g^\circ(\gamma j)$. En effet, si les séquences complétées s'écrivaient sous la forme

$$i'2\ldots2j', \quad i''2\ldots2j'' \tag{4}$$

avec les j', j'' différents, le premier changement du chiffre j' dans la suite $\Gamma_g^\circ(\gamma j)$ (sans tilde) pendant le traitement de la séquence $i'2\ldots2j'$ se présenterait comme suit :

$$i'''2\ldots21j' \xrightarrow{a} i'''2\ldots21j''$$

(compte tenu du mécanisme d'action des automates a et b, voir les exercices 23.2.1 et 23.2.2); il y aurait donc dans $\widetilde{\Gamma}^{\circ}_{g}(\gamma)$ la séquence $i^{m}2 \ldots 21$ entre les séquences (4), ce qui est faux. Ainsi donc, tant que le chiffre caudal 2 reste inchangé dans la suite $\widetilde{\Gamma}^{\circ}_{g}(\gamma)$, le nouveau chiffre caudal — ajouté — des termes correspondants de la suite $\widetilde{\Gamma}^{\circ}_{g}(\gamma j)$ reste inchangé, lui aussi.

Ceci noté, considérons d'abord le cas où $g^{d}/\gamma \sim \varepsilon$. On a alors $(\gamma j)\, g^{d} = \gamma j$, c'est pourquoi $\widetilde{\Gamma}_{g}(\gamma j)$ a la même longueur que $\widetilde{\Gamma}_{g}(\gamma)$ et se déduit de cette dernière en mettant 1 ou 2 après les termes de la forme $i2 \ldots 2$. De la remarque précédente et d'un raisonnement combinatoire facile, il ressort que pour $\mathrm{sgm}^{\circ}_{g}(\gamma) \geqslant 2$ on a $\mathrm{sgm}^{\circ}_{g}(\gamma j) \leqslant \left[\frac{1}{2}\,\mathrm{sgm}^{\circ}_{g}(\gamma)\right]$. Puisque pour $m = 1, 2, \ldots$ on a évidemment $\left[\frac{m}{2}\right] < m$, l'inégalité (3) a lieu pour $\mathrm{fl}_{g}(\gamma) > 0$.

Soit maintenant $g^{d}/\gamma \sim \tau$. Alors $(\gamma j)\, g^{d} = \gamma j^{\tau}$, $(\gamma j)\, g^{2d} = \gamma j$, i.e. $\widetilde{\Gamma}_{g}(\gamma j)$ est deux fois plus longue que $\widetilde{\Gamma}_{g}(\gamma)$. Etant donné qu'aux 1-segments connexes dans la première moitié de la suite $\widetilde{\Gamma}_{g}(\gamma j)$ correspondent des 2-segments connexes, et inversement, on calcule la flexibilité, par rapport à g, de la séquence γ à l'aide du tableau suivant:

type des remuements de la queue dans les moitiés de $\widetilde{\Gamma}_{g}(\gamma j)$		m = nombre total des segments dans chaque moitié	$\mathrm{sgm}^{\circ}_{g}(\gamma j)$
dans la première	dans la seconde		
$1 \sim 1$	$2 \sim 2$	impair	m
$1 \sim 2$	$2 \sim 1$	pair	$m-1$
$2 \sim 1$	$1 \sim 2$	pair	$m-1$
$2 \sim 2$	$1 \sim 1$	impair	m

Nous voyons dans tous les cas que

$$\mathrm{fl}_{g}(\gamma j) = \left[\frac{1}{2}\,\mathrm{sgm}^{\circ}_{g}(\gamma j)\right] = \left[\frac{m-1}{2}\right].$$

Puisque

$$m \leqslant \mathrm{sgm}_{g}(\gamma) \leqslant \mathrm{sgm}^{\circ}_{g}(\gamma) + 1,$$

l'inégalité (2) est vérifiée dans tous les cas.

e) Pour tout $g \in G$ il existe un entier naturel n_{g} tel que la flexibilité par rapport à g de toute séquence de longueur n_{g} reste inchangée,

quels que soient les chiffres qu'on puisse ajouter à la fin de la séquence, i.e.

$$\mathrm{fl}_g\ (\gamma\eta) = \mathrm{fl}_g\ (\gamma)$$

pour toute γ de longueur n_g et toute séquence η.

En effet, l'ensemble I^n de toutes les séquences de longueur n de l'alphabet $I = \{1, 2\}$ se décompose en orbites par rapport au groupe cyclique (g); appelons-les *n-orbites*. Il est clair que les segments initiaux de longueur $n' < n$ des séquences d'une n-orbite quelconque N appartiennent eux-mêmes à une même orbite; de plus, ils constituent exactement une n'-orbite N'. Nous dirons que la n-orbite N *prolonge* la n'-orbite N'. En accord avec l'exercice 23.2.4, à chaque n-orbite N on peut associer sa *flexibilité* $\mathrm{fl}\ (N) = \mathrm{fl}_g(\gamma)$, $\gamma \in N$.

Supposons que l'ensemble I^3 se décompose en 3-orbites $I_1^3, \ldots, I_r^3$ et que $\mathrm{fl}(I_k^3) = f_k^3$. Soient $\gamma_1 \in I_1^3$ et d_1 le plus petit nombre tel que $\gamma_1 g^{d_1} = \gamma_1$. Si $g^{d_1}/\gamma_1 \sim \varepsilon$, on a

$$(\gamma_1 j)\ g^{d_1} = \gamma_1 j, \quad \mathrm{fl}_g\ (\gamma_1 j) < \mathrm{fl}_g(\gamma_1)$$

pour tout $j \in \{1, 2\}$ (voir d)); il y a donc dans I^4 deux 4-orbites I_1^4, I_2^4 qui prolongent I_1^3 et qui ont une flexibilité plus petite que $\mathrm{fl}\ (I_1^3)$. Au contraire, si $g^{d_1}/\gamma_1 \sim \tau$, il n'y a dans I^4 qu'une seule 4-orbite I_1^4 prolongeant I_1^3, et ceci en sorte que $\mathrm{fl}\ (I_1^4) \leqslant \mathrm{fl}\ (I_1^3)$. Poursuivant ce processus par récurrence, nous nous assurons que pour tout $n = 4, 5, \ldots$ ou bien il existe une n-orbite unique prolongeant la $(n - 1)$-orbite donnée, ou bien il y en a deux mais de flexibilité strictement inférieure à celle de la $(n - 1)$-orbite donnée. Puisque le nombre r de $f_1^3, \ldots, f_r^3$ est fini, on réussit à obtenir un n_g tel que chaque $(n_g - 1)$-orbite est couverte exactement par une n_g-orbite et la flexibilité cesse de diminuer. Cela confirme notre proposition.

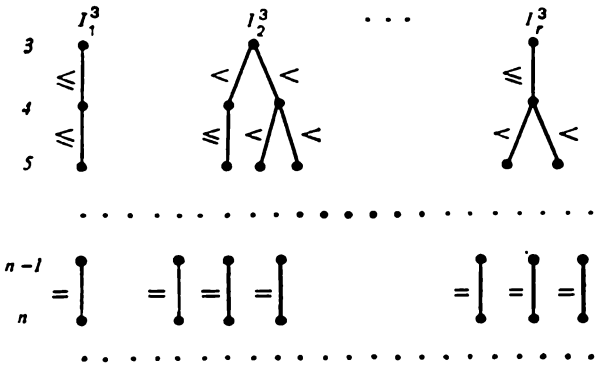
Le schéma ci-après illustre ce raisonnement: les orbites sont représentées par des points, et leurs prolongements, par des segments allant de haut en bas.

Nous verrons plus tard que la stabilisation de la flexibilité décrite sous e) a toujours lieu au niveau du zéro; or, pour le démontrer, nous aurons besoin d'une nouvelle notion auxiliaire, à savoir: le type de la suite $\tilde{\Gamma}_g\ (\gamma)$.

f) Soit de nouveau $\gamma g^d = \gamma$, long. $\gamma \geqslant 3$. Quelle doit être la permutation g^d/γ? Il est possible de donner une réponse bien déterminée à cette question en imposant certaines restrictions à long. γ. En effet, soit $T = \{1\}$, $\{2\}$ ou $\{1, 2\}$. En vertu de la formule établie dans l'exercice 23.2.1, il existe un nombre aussi grand que l'on veut n_T tel que pour toute séquence δ

$$a/\delta \sim \tau \Longleftrightarrow \delta = i2 \ldots 21, \quad i \in T.$$

Donc, si long. $\gamma = n_T$ et N_T est le nombre de toutes les séquences



de la forme $i2 \ldots 21$, $i \in T$, dans la suite $\widetilde{\Gamma}_g(\gamma)$, on a

$$g^d/\gamma \sim \tau^{N_T}.$$

En particulier, on a $g^d/\gamma \sim \varepsilon$ si et seulement si N_T est pair. Vu l'importance attachée à ce cas précis, introduisons une terminologie appropriée: nous dirons que T est le *type* de la suite $\widetilde{\Gamma}_g(\gamma)$ si le nombre N_T est pair.

23.2.5. Exercice. Pour g, γ quelconques la suite $\widetilde{\Gamma}_g(\gamma)$ admet au moins un type (et peut-être plusieurs). (A noter que l'un au moins parmi les nombres N_1, N_2, $N_1 + N_2$ est nécessairement pair.)

g) Montrons que si, en ajoutant des chiffres à la fin des séquences, la flexibilité par rapport à un g se stabilisait ailleurs que sur zéro, il y aurait stabilisation des types pas plus tard que sur le pas immédiatement postérieur à la stabilisation de la flexibilité. Plus exactement, si

$$0 < \mathrm{fl}_g(\gamma) = \mathrm{fl}_g(\gamma j_1) = \mathrm{fl}_g(\gamma j_1 j_2)$$

pour une séquence γ et deux chiffres j_1, j_2, les types des suites $\widetilde{\Gamma}_g(\gamma j_1)$, $\widetilde{\Gamma}_g(\gamma j_1 j_2)$ sont les mêmes.

En effet, soit d le plus petit nombre tel que $\gamma g^d = \gamma$. En vertu de la première égalité et de la remarque d), on a $g^d/\gamma \sim \tau$, aussi la suite $\widetilde{\Gamma}_g(\gamma j_1)$ doit-elle comprendre, pour chaque séquence de la forme $\delta 1$, une séquence de la forme $\delta 2$, et inversement (voir le troisième alinéa de d)). Pour la même raison, la suite $\widetilde{\Gamma}_g(\gamma j_1 j_2)$ doit contenir, pour chaque séquence $\delta 1$, une séquence $\delta 2$, et inversement. Il est donc possible de déduire l'ensemble des séquences de $\widetilde{\Gamma}_g(\gamma j_1 j_2)$ de chiffre

caudal 1 à partir des séquences analogues de $\widetilde{\Gamma}_g(\gamma j_1)$ en substituant 2 au chiffre caudal 1 et en ajoutant à la fin un nouveau chiffre caudal 1. La proposition résulte alors immédiatement de la définition du type (voir f)).

h) Montrons que la stabilisation de la flexibilité décrite sous e) a effectivement toujours lieu au niveau du zéro, i.e. que $\mathrm{fl}_g(\gamma) = 0$ pour toute γ de longueur $\geqslant n_g$.

En effet, on a d'après e)

$$\mathrm{fl}_g(\gamma) = \mathrm{fl}_g(\gamma\eta)$$

pour toutes les γ de longueur n_g et pour toutes les η. Supposons que $\mathrm{fl}_g(\gamma) > 0$. En vertu de g), toutes les suites

$$\widetilde{\Gamma}_g(\gamma j_1 \ldots j_k), \quad k = 1, 2, \ldots$$

admettent les mêmes types pour n'importe quels $j_1, j_2, \ldots$ de $\{1, 2\}$; soit T un de ces types. Conformément à f), il existe un $n'_g > n_g$ tel que pour toute séquence δ de longueur n'_g on a

$$a/\delta \sim \tau \leftrightharpoons \delta = i2 \ldots 21, \quad i \in T.$$

Posons $k = n'_g - n_g$; on a alors long. $\gamma j_1 \ldots j_k = n'_g$. Soit un d tel que $(\gamma j_1 \ldots j_k)\, g^d = \gamma j_1 \ldots j_k$. Puisque le nombre N_T de toutes les séquences de la forme $i2 \ldots 21$, $i \in T$, dans la suite $\widetilde{\Gamma}_g(\gamma j_1 \ldots j_k)$ est pair (par définition du type), on a $g^d/\gamma j_1 \ldots j_k \sim \varepsilon$ (voir f)). Or, il doit y avoir alors, en vertu de d), l'inégalité stricte

$$\mathrm{fl}_g(\gamma j_1 \ldots j_{k+1}) < \mathrm{fl}_g(\gamma j_1 \ldots j_k)$$

manifestement contraire à l'hypothèse.

i) Montrons enfin que le groupe G est périodique. Plus exactement, si $g \in G$, on a $g^{2^{n_g+2}} = 1$, où $n_g \geqslant 3$ est le nombre défini sous e) (voir aussi le n° précédent). Tout d'abord nous savons déjà (voir b)) que si $d = 2^{n_g}$, on a $\gamma g^d = \gamma$ pour toute séquence γ de longueur n_g. Il reste à montrer que

$$(\gamma\eta)\, g^{4d} = \gamma\eta \quad \text{pour } \eta \text{ quelconque.}$$

Puisque $\mathrm{fl}_g(\gamma) = 0$, quatre cas sont à distinguer ici :

1° La suite $\widetilde{\Gamma}^\circ_g(\gamma)$ est vide. En particulier, elle ne contient alors aucune séquence de la forme $i2 \ldots 21$. Puisque l'automate a ne fait changer que le chiffre ajouté à la fin d'une telle séquence et que l'automate b ne fait changer aucun chiffre à partir de la troisième position, on a $(\gamma j)\, g^d = \gamma j$ pour tout $j \in \{1, 2\}$. Puisque $\widetilde{\Gamma}^\circ_g(\gamma)$ ne contient aucune séquence de la forme $i2 \ldots 2$ non plus, la suite $\widetilde{\Gamma}^\circ_g(\gamma j)$ est vide, elle aussi. En répétant ce raisonnement, on obtient donc $(\gamma\eta)\, g^d = \gamma\eta$ pour une séquence η quelconque.

2° La suite $\widetilde{\Gamma}_g^\circ(\gamma)$ ne contient que des séquences de la forme $i2\ldots21$. Soit $j \in \{1, 2\}$. Puisque $\widetilde{\Gamma}_g^\circ(\gamma j)$ ne peut comprendre aucune séquence qui ne soit déjà dans $\widetilde{\Gamma}_g(\gamma)$ par son segment initial, la suite $\widetilde{\Gamma}_g^\circ(\gamma j)$ est vide. Puisque $\gamma g^d = \gamma$, on a $(\gamma j)\, g^{2d} = \gamma j$, et l'on retrouve le cas 1° pour la séquence γj.

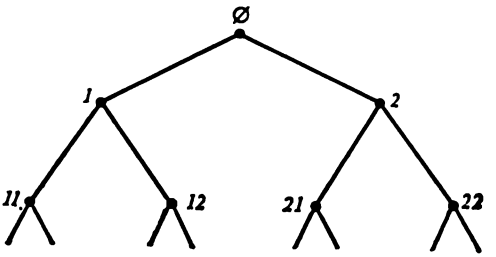
3° La suite $\widetilde{\Gamma}_g^\circ(\gamma)$ ne contient que des séquences de la forme $i2\ldots2$. De même que dans le cas 1°, il s'ensuit que $(\gamma j)\, g^d = \gamma j$ pour tout chiffre $j \in \{1, 2\}$. Il y a plus: la suite $\widetilde{\Gamma}_g^\circ(\gamma j)$ s'obtient à partir de $\widetilde{\Gamma}_g^\circ(\gamma)$ en y ajoutant le même chiffre j. Si $j = 1$, on retrouve le cas 2° pour la séquence γj, et la proposition est démontrée. Si par contre $j = 2$, on retrouve le cas 3° étudié ci-dessus mais déjà pour γj. Il vient comme précédemment

$$(\gamma 21\eta)\, g^{2d} = \gamma 21\eta, \quad (\gamma 22)\, g^d = \gamma 22,$$

et ainsi de suite.

4° La suite $\widetilde{\Gamma}_g^\circ(\gamma)$ se compose d'un 1-segment et d'un 2-segment. Alors pour tout $j \in \{1, 2\}$ la suite $\widetilde{\Gamma}_g^\circ(\gamma j)$ nous fait retrouver soit le cas 2°, soit le cas 3°. Etant donné que $(\gamma j)\, g^{2d} = \gamma j$, on a $(\gamma j\eta)\, g^{4d} = \gamma j\eta$ pour une séquence η quelconque. Le théorème est démontré.

23.3. Autre démonstration. Introduisons dans l'ensemble K_2^ω de toutes les séquences de l'alphabet $\{1, 2\}$ la relation d'ordre partiel $\leqslant$ en posant $\gamma \leqslant \delta$ si γ est le segment initial de la séquence δ. Représentons les séquences de même longueur par des points situés à la même hauteur et les séquences de longueur plus grande par des points situés plus bas et relions γ à δ par un segment chaque fois que $\gamma \leqslant \delta$; nous obtenons la représentation canonique de l'ensemble K_2^ω sous la forme d'un arbre:



Il est clair que les transformations séquentielles conservent la relation $\leqslant$, ce qui fait que le groupe d'Aliochine $G = \mathrm{gr}\,(a, b)$ se plonge naturellement dans le groupe $\mathrm{Aut}\, K_2^\omega$ des automorphismes de l'arbre K_2^ω.

23.3.1. Exercice. Soient p un nombre premier et K_p^n l'ensemble des séquences de longueur $\leqslant n$ de l'alphabet $\{1, 2, \ldots, p\}$, muni de la relation d'ordre partiel définie plus haut (un tel ensemble est appelé *arbre de multiplicité p et de hauteur n*). Alors

$$\mathrm{Aut}\, K_p^n \simeq \underbrace{\mathbb{Z}_p \wr (\ldots \wr (\mathbb{Z}_p \wr \mathbb{Z}_p) \ldots)}_{n \text{ fois}}.$$

Si $K_p^\omega = \bigcup_{n=1}^{\infty} K_p^n$ (arbre de toutes les séquences), alors Aut K_p^ω est la réunion de la suite de groupes $G_p^n = \mathrm{Aut}\, K_p^n$ dont chacun se plonge naturellement dans le suivant: $G_p^n \to G_p^{n+1} = \mathbb{Z}_p \wr G_p^n$, ce qui permet de considérer les groupes de transformations séquentielles comme des sous-groupes de cette réunion G_p^ω. On trouve des constructions analogues à celles de S.V. Aliochine mais exposées dans le langage des arbres, y compris la démonstration, dans les travaux de V.I. Souchtchanski (voir par exemple *DAN SSSR*, 1979, **247**, n° 3, p. 557-561).

Comment l'automate a opère-t-il sur l'arbre K_2^ω? Rappelons que si long. $\gamma \geqslant 3$, on a $a/\gamma \sim \tau$ si et seulement si

$$\gamma = 12 \ldots 21 \text{ et long. } \gamma \equiv 0 \text{ ou } 2 \pmod 3$$

ou

$$\gamma = 22 \ldots 21 \text{ et long. } \gamma \equiv 1 \text{ ou } 2 \pmod 3$$

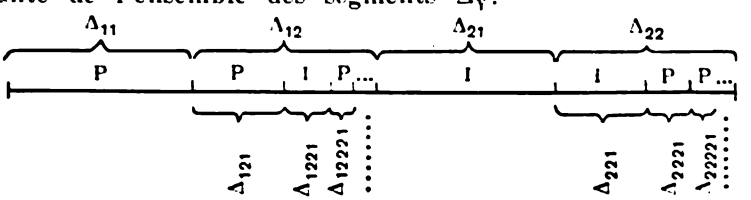
(voir l'exercice 23.2.1). Donc, l'automate a opère sur les sous-arbres $[\gamma]$ aux « racines » γ de la forme indiquée par la transformation

$$P: \gamma 1 \eta \leftrightarrow \gamma 2 \eta$$

(la *permutation des moitiés*), et sur tous les autres sous-arbres $[\delta]$, par la transformation identique

$$I: \delta\eta \leftrightarrow \delta\eta.$$

Considérons encore une interprétation naturelle de l'ensemble K_2^ω. Soit Δ un segment de droite, soient Δ_1, Δ_2 ses moitiés, soient Δ_{11}, Δ_{12}, Δ_{21}, Δ_{22} les moitiés de ces dernières, et ainsi de suite. La séquence γ sera représentée par le segment Δ_γ. Désignons par P la permutation des moitiés (la gauche va à droite, la droite à gauche) et par I la transformation identique du segment. On comprend sans difficulté que l'automate a se traduit dans ce langage par la transformation suivante de l'ensemble des segments Δ_γ:

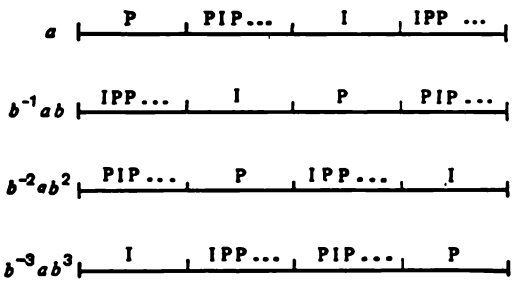


Plus exactement, sur le premier quart Δ_{11} de Δ la transformation a se présente comme P, tandis que sur le deuxième quart Δ_{12} elle consiste à partager Δ_{12} en deux moitiés, à partager sa seconde moitié encore une fois en deux moitiés, la seconde moitié obtenue encore en deux moitiés, et ainsi de suite, et à distribuer ensuite sur les segments obtenus les transformations PIPPIP... Sur le troisième quart Δ_{21} la transformation a agit comme I, tandis que le quatrième quart Δ_{22} est de nouveau partagé comme le deuxième et les transformations IPPIPP... sont distribuées sur les segments obtenus.

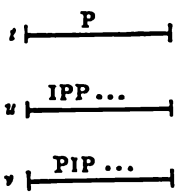
Soit G_0 un sous-groupe de G constitué par des éléments qui se laissent exprimer au moyen des générateurs a, b, la somme des exposants de b étant nulle. Il est clair que $|G : G_0| = 4$ (les représentants dans les classes suivant G_0 étant 1, b, b^2, b^3) et

$$G_0 = \mathrm{gr}\,(a,\ b^{-1}ab,\ b^{-2}ab^2,\ b^{-3}ab^3).$$

23.3.2. Exercice. Vérifier que les éléments générateurs du groupe G_0 opèrent sur les quarts du segment Δ de la façon suivante :



Soit maintenant Γ un autre segment de droite ; soient t, u, v les transformations de l'ensemble de ses parties 2-aires, définies par les schémas



(pour u, v on sous-entend le partage « seconde moitié en deux » décrit plus haut). Soit

$$H = \mathrm{gr}\,(t,\ u,\ v).$$

Il est clair que G_0 est le produit sous-direct de quatre exemplaires du groupe H (voir l'exercice 23.3.2); donc, G est un 2-groupe infini si et seulement si H l'est. Ainsi donc, nous allons avoir une démonstration alternative au théorème de S.V. Aliochine 23.2.3 (en omettant cependant le fait que G se laisse approcher par des 2-groupes finis, qui se démontre sans difficulté dans la première variante), à condition de démontrer un nouveau

23.3.3. Théorème (R.I. Grigortchouk). *Le groupe H est un 2-groupe infini.*

Il est remarquable que nous obtiendrons en passant encore un exemple de groupe périodique qui n'est pas localement fini et qui est inclus dans le groupe d'Aliochine à titre de section.

Démonstration. Il est évident que $uv = w$, où w est illustré par

On vérifie immédiatement que

$$t^2 = u^2 = v^2 = w^2 = 1,$$

$$uv = vu = w, \quad uw = wu = v, \quad vw = wv = u,$$

aussi tout élément de H s'écrit-il

$$*t*t* \ . \ . \ . *t*,$$

où les étoiles symbolisent des éléments de la forme u, v, w (elles peuvent être absentes aux extrémités). Soit H_0 un sous-groupe de H composé d'éléments qui se laissent écrire avec un nombre pair de facteurs t. Il est évident que $|H : H_0| = 2$,

$$H_0 = \mathrm{gr}\,(tut,\ tvt,\ twt,\ u,\ v,\ w)$$

et que H_0 applique chacune des deux moitiés Γ_1, Γ_2 du segment Γ sur elle-même. Soit φ_i la restriction de H_0 à Γ_i. On vérifie sans peine que les homomorphismes φ_1, φ_2 opèrent sur les éléments générateurs du groupe H_0 comme suit:

x	tut	tvt	twt	u	v	w
x^{φ_1}	$\tilde{w}$	$\tilde{u}$	$\tilde{v}$	1	$\tilde{t}$	$\tilde{t}$
x^{φ_2}	1	$\tilde{t}$	$\tilde{t}$	$\tilde{w}$	$\tilde{u}$	$\tilde{v}$

(5)

(le tilde est mis pour souligner que la transformation correspondante ne se rapporte déjà plus à Γ). Il est important que t o u s les éléments t, u, v, w apparaissent maintenant sous le tilde, si bien que

$$H_0^{\varphi_1} \simeq H_0^{\varphi_2} \simeq H.$$

Puisque $x \longmapsto x^{\varphi_1} \times x^{\varphi_2}$ définit une injection de H_0, le groupe H apparaît comme image homomorphe de son propre sous-groupe H_0. Autrement dit, H est infini.

Montrons à présent que l'ordre de son élément quelconque est de la forme 2^m. Cela est évident pour les générateurs t, u, v, w: nous opérons donc par récurrence sur k = long. h. Supposons démontré que les éléments de longueur plus petite que k ont les ordres de la forme 2^m. On admet que $k \geqslant 2$ et que h se laisse mettre sous la forme spéciale

$$h = t*t* \ldots *t*, \tag{6}$$

où les étoiles désignent comme précédemment u, v, w (sinon nous aurions conjugué h par l'élément t ou $*$).

1er cas. On a $h \in H_0$. Le produit (6) se décompose alors en quadruplets $t*t*$. En regardant le tableau (5), on remarque que chaque quadruplet de ce type se transforme en $\widetilde{*t}$, $\widetilde{t*}$ ou $\widetilde{*}$ sous l'action de φ_1 et φ_2, si bien que

$$\text{long. } h^{\varphi_i} \leqslant \frac{k}{2} < k.$$

Par hypothèse de récurrence, h^{φ_1}, h^{φ_2} sont des 2-éléments, donc h est un 2-élément, lui aussi.

2e cas. On a $h \notin H_0$ et il y a au moins un facteur u dans la notation (6). Quitte à faire une conjugaison convenable, on suppose que u est précisément la première étoile. Puisque $|H : H_0| = 2$, on a $h^2 \in H_0$; en outre, h^2 commence par le quadruplet $tut*$ et contient en son milieu le quadruplet $t*tu$. En regardant le tableau (5), on remarque que $t*tu$ se transforme en $\widetilde{*}$ sous l'action de φ_1, et que $tut*$ se transforme en $\widetilde{*}$ sous l'action de φ_2. Par conséquent,

$$\text{long. } (h^2)^{\varphi_1} < k, \quad \text{long. } (h^2)^{\varphi_2} < k,$$

et il ne reste qu'à évoquer l'hypothèse de récurrence.

3e cas. On a $h \in H_0$, il n'y a aucun facteur u dans (6) mais il y a au moins un facteur v. Quitte à faire une conjugaison convenable, on admet que v est précisément la première étoile. On a de nouveau $h^2 \in H_0$, mais cette fois-ci h^2 commence par le quadruplet $tvt*$ et admet en son milieu le quadruplet $t*tv$. En regardant le tableau (5), on remarque que $tvt*$ se transforme en $\widetilde{ut}$ sous l'action de φ_1, tandis

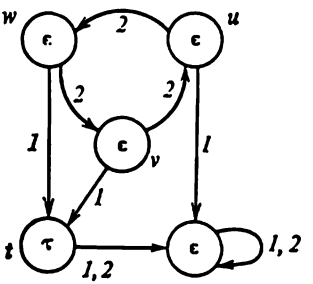
que $t*tv$ se transforme en $\widetilde{tu}$ sous l'action de φ_2, aussi les deux mots $(h^2)^{\varphi_i}$ contiennent-ils, dans leurs notations, un facteur u. Puisque

$$\text{long. } (h^2)^{\varphi_1} \leqslant k, \quad \text{long. } (h^2)^{\varphi_2} \leqslant k, \tag{7}$$

on se retrouve dans le 2^e cas que l'on vient d'examiner.

4^e cas. On a $h \notin H_0$ et il n'y a ni u ni v dans (6). On a alors $h^2 \in H_0$ et h^2 commence par le quadruplet $twtw$. En regardant le tableau (5), on remarque que ce quadruplet se transforme en $\widetilde{vt}$ sous l'action de φ_1 et en $\widetilde{tv}$ sous l'action de φ_2, si bien que les deux mots $(h^2)^{\varphi_i}$ admettent dans leurs notations un facteur v. Les inégalités (7) étant vérifiées comme précédemment, on retrouve le 3e cas ci-dessus. Le théorème est démontré.

23.3.4. Exercice. Assimilant les générateurs t, u, v, w du groupe H à des transformations de l'ensemble K_2^ω des séquences de l'alphabet $\{1, 2\}$, on peut les définir à l'aide des automates suivants :



Tous les quatre automates sont représentés à l'aide d'un seul schéma, car ils ne diffèrent que par les états initiaux (marqués par la lettre correspondante). En le comparant avec l'automate d'Aliochine a, on voit nettement comment le groupe H se laisse introduire dans le groupe d'Aliochine en tant que section.

§ 24. Conditions minimale et maximale

24.1. Définitions et exemples. On dit que le groupe vérifie la *condition maximale* (*pour ses sous-groupes*) ou est *artinien* si toute série décroissante de ses sous-groupes $H_1 \geqslant H_2 \geqslant \ldots$ devient stationnaire, i.e. $H_n = H_{n+1} = \ldots$ à partir d'un certain n. On dit que le groupe vérifie la *condition maximale* (*pour ses sous-groupes*) ou est *nœthérien* si toute série croissante de ses sous-groupes $H_1 \leqslant H_2 \leqslant \ldots$ devient stationnaire, i.e. $H_n = H_{n+1} = \ldots$ à partir d'un certain n.

Il va sans dire que tout groupe vérifiant la condition minimale doit être périodique, car un groupe cyclique infini ne vérifie pas cette condition.

24.1.1. E x e r c i c e. La condition maximale revient à demander que tous les sous-groupes du groupe considéré soient de type fini.

24.1.2. E x e r c i c e. Les conditions minimale et maximale sont conservées en passant aux sous-groupes, aux images homomorphes et aux extensions.

Compte tenu de cet exercice et de la remarque évidente selon laquelle le groupe quasi cyclique C_{p^∞} vérifie la condition minimale (voir l'exercice 2.4.10) et le groupe cyclique infini $\mathbb{Z}$ la condition maximale, nous obtenons un exemple fondamental qui suit.

24.1.3. E x e m p l e. On appelle *groupe de Tchernikov* l'extension du produit direct d'un nombre fini de groupes quasi c y cliques (suivant des nombres premiers distincts en général) par un groupe fini (par produit de zéro facteurs, on sous-entend ici le groupe unité). Tout groupe de Tchernikov vérifie la condition minimale. Tout groupe presque polycyclique vérifie la condition maximale.

Quelque invraisemblable que cela puisse paraître, mais on ignorait encore tout récemment si cet exemple canonique couvre tous les groupes vérifiant la condition minimale (problème de Tchernikov) et tous les groupes vérifiant la condition maximale (problème de Baer), bien que l'intérêt suscité par ces deux problèmes ne cessât de croître pendant les décennies qui apportaient des réponses positives dans une classe de groupes après l'autre. La réponse définitive fut cependant négative dans les deux cas, ce que montre l'exemple de A.Iou. Olchanski (voir § 2). La découverte de pareils exemples aura mis la dernière touche au tableau des résultats positifs obtenus antérieurement. Nous en mentionnerons deux, qui sont les plus significatifs: les groupes localement résolubles vérifiant la condition minimale pour les sous-groupes abéliens sont des groupes de Tchernikov (S.N. Tchernikov in: *Matem. sb.*, 1951, 28, n° 1, p. 119-129); les groupes localement finis vérifiant la même condition sont des groupes de Tchernikov (V.P. Chounkov in: *Alguebra i loguika*, 1970, 9, § 5, p. 579-615). Le premier résultat sera démontré dans le texte (théorème 24.3.4); quant au second, sa démonstration est fondée malheureusement sur des renseignements trop spéciaux de la théorie des groupes finis simples et reste donc trop encombrante pour trouver sa place dans un ouvrage d'enseignement.

Les groupes résolubles vérifiant la condition minimale trouvent leur description complète dans le

24.1.4. T h é o r è m e (S.N. Tchernikov). *Tout groupe résoluble G vérifiant la condition minimale est un groupe de Tchernikov* (ou, selon la terminologie proposée par S.N. Tchernikov, *un groupe extrémal*).

D é m o n s t r a t i o n. En vertu de la condition minimale, le groupe G contient un sous-groupe d'indice fini H qui, lui, ne contient

aucun sous-groupe d'indice fini. Puisque l'intersection de deux sous-groupes d'indice fini est encore d'indice fini, H est unique, donc normal. Si H est abélien, le groupe quotient $H/H^p \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots$ est fini pour tout p premier, donc $H = H^p$, i.e. H est un groupe abélien complet. Conformément au théorème 9.1.6, il se décompose en produit direct de groupes quasi cycliques. En vertu de la condition minimale, leur nombre est fini. Le théorème est donc démontré pour G abélien.

Supposons à présent que G soit un groupe infini non abélien. Choisissons dans H un sous-groupe normal abélien non trivial A (par exemple, le dernier commutant distinct de l'unité). Montrons que A est contenu dans le centre de H. En effet, A est un groupe abélien vérifiant la condition minimale; il ne contient donc, en vertu de ce qui précède, qu'un nombre fini d'éléments de chaque ordre donné. Cela revient à dire que tout élément a de A admet un nombre fini de conjugués dans H, d'où $|H : C_H(a)| < \infty$. Puisque H ne contient aucun sous-groupe d'indice fini, on a

$$C_H(a) = H, \quad A \leqslant Z(H),$$

ce qu'il fallait démontrer.

Montrons maintenant que le sous-groupe H est nilpotent. Raisonnons par récurrence sur son degré de résolubilité k. Puisqu'on a en vertu de ce qui précède $H^{(k-1)} \leqslant Z(H)$, le groupe quotient $H/Z(H)$ est résoluble de degré $\leqslant k-1$. Par hypothèse de récurrence appliquée à $G/Z(H)$, le groupe $H/Z(H)$ est nilpotent; il en est donc de même pour H.

Montrons enfin que H est abélien. Soit B un sous-groupe normal abélien maximal dans H. En vertu de ce que nous venons de montrer, B est contenu dans le centre de H; en vertu du théorème 16.2.6, il se confond avec son centralisateur dans H. D'où $B = H$, i.e. H est abélien. Le théorème est démontré.

24.1.5. Exercice. La classe des groupes de Tchernikov est fermée pour la prise de sous-groupes, d'images homomorphes et d'extensions.

Puisque les automorphismes des groupes de la forme

$$\mathbb{C}_{p^\infty} \times \ldots \times \mathbb{C}_{p^\infty}$$

se représentent par des matrices de $\mathrm{GL}_n(\mathbb{Z}_{p^\infty})$ (exercice 5.1.4), l'étude des groupes de Tchernikov se trouve grandement facilitée par le résultat suivant:

24.1.6. Exercice. Le groupe de matrices $\mathrm{GL}_n(\mathbb{Z}_{p^\infty})$ est presque sans torsion. En particulier, ses sous-groupes périodiques sont finis.

I n d i c a t i o n. Le sous-groupe de congruence modulo p^i, $i = 1, 2, \ldots$, i.e. le groupe des matrices $e + p^i a$, $a \in M_n(\mathbb{Z}_{p^\infty})$, est d'indice fini dans $GL_n(\mathbb{Z}_{p^\infty})$ et est sans torsion, à l'exception du cas $p = 2$, $i = 1$ (voir les exercices 4.2.7 et 5.1.5).

En ce qui concerne les groupes résolubles vérifiant la condition maximale, ils trouvent leur description complète dans le simple théorème que voici:

24.1.7. T h é o r è m e. *Un groupe G est résoluble et vérifie la condition maximale si et seulement s'il est polycyclique.*

D é m o n s t r a t i o n. Nous avons déjà vu que la condition est suffisante (voir l'exemple 24.1.3). Montrons que la condition est nécessaire. Supposons que G vérifie la condition maximale et admet une matriochka résoluble finie

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G.$$

Puisque ses sections G_{i+1}/G_i vérifient la condition maximale, elles aussi (voir l'exercice 24.1.2), elles sont de type fini et se décomposent donc en produits directs de groupes cycliques (théorème 8.1.2). Cela permet de subdiviser la matriochka donnée de façon à obtenir une matriochka polycyclique. Le théorème est démontré.

En démontrant les théorèmes 24.1.4 et 24.1.7, nous avons décrit les groupes a b é l i e n s vérifiant les conditions minimale et maximale. Cette description, qui revêt une importance capitale, mérite d'être mentionnée à part:

24.1.8. E x e r c i c e. Un groupe abélien vérifie la condition minimale si et seulement s'il se décompose en produit direct d'un nombre fini de groupes quasi cycliques et de groupes cycliques finis. En particulier, tout p-groupe abélien vérifiant la condition minimale est nécessairement de rang fini (voir le théorème 10.1.16). Un groupe abélien vérifie la condition maximale si et seulement s'il se décompose en produit direct d'un nombre fini de groupes cycliques.

24.1.9. E x e r c i c e. Compte tenu du théorème local de A.I. Maltsev 22.3.2 et du théorème de O.Iou. Schmidt 23.1.1, généraliser le théorème 24.1.4 sans modifier le schéma de sa démonstration: *tout RN-groupe vérifiant la condition minimale est un groupe résoluble de Tchernikov.*

24.2. Passage des sous-groupes abéliens au groupe résoluble. Nous nous proposons de montrer, dans ce n°, que la condition minimale ou maximale vérifiée pour les sous-groupes abéliens d'un groupe résoluble G est toujours vérifiée pour ses sous-groupes quelconques, ce qui veut dire que G est comme précédemment un groupe de Tcher-

nikov ou un groupe polycyclique, selon le cas. La première chose qui vient à l'esprit est bien sûr la démonstration par récurrence sur le degré de résolubilité. Soit A le dernier commutant non trivial de G. Si nous réussissons à montrer que tous les sous-groupes abéliens dans G/A vérifient à leur tour la condition minimale (resp. maximale), il ne restera qu'à nous rappeler qu'un groupe de Tchernikov (resp. polycyclique) reste tel dans toutes les extensions (voir les exercices 4.4.3 et 24.1.5). On veut donc apprendre à montrer qu'une propriété des sous-groupes de G reste vraie quand on passe au groupe quotient de G par son sous-groupe normal abélien A. Ne pourrait-on pas « greffer » les sous-groupes de G/A sur G lui-même, afin que leurs propriétés soient héritées ? L'idéal, ce serait que A admette un supplémentaire dans G, i.e. qu'il y ait dans G un sous-groupe X tel que

$$G = XA, \quad X \cap A = 1$$

(auquel cas l'on aurait $X \simeq G/A$). Nous allons voir que si l'idéal n'est pas toujours accessible, on peut en revanche garantir une « presque supplémentarité » qui sera justement notre outil principal.

Soit A un sous-groupe normal dans G. Nous dirons que A est min-*irréductible* par rapport à G si tout sous-groupe normal H de G, contenu dans A et distinct de A est fini. Par dualité, nous dirons que A est max-*irréductible* par rapport à G si, pour tout sous-groupe normal H de G contenu dans A et distinct de 1, le groupe quotient A/H est périodique. (Une dualité parfaite consisterait bien sûr à demander que A/H soit fini. Or, dans les applications, la max-irréductibilité intervient le plus souvent sous cette forme affaiblie ; cela explique d'ailleurs pourquoi, dans le lemme qui va suivre, nous faisons plus de conjectures pour le cas de groupe max-irréductible et pourquoi la démonstration de ce cas est plus longue.)

24.2.1. Lemme. *Soit $A \trianglelefteq G$; soient A, G/A tous deux abéliens ; soit A non central dans G.*

a) *Si A est* min-*irréductible par rapport à G, il existe un sous-groupe X tel que*

$$G = XA \quad et \quad |X \cap A| < \infty.$$

b) *Si A est un groupe sans torsion de rang fini,* max-*irréductible par rapport à G, il existe un sous-groupe X tel que*

$$|G : XA| < \infty \quad et \quad X \cap A = 1.$$

Démonstration. On peut admettre d'emblée que le sous-groupe A est infini, sinon l'on aurait le cas a) et il suffirait de prendre $X = G$. Choisissons dans G un élément x tel que $[A, x] \neq 1$ et montrons que son centralisateur $X = C_G(x)$ est le sous-groupe cherché dans les deux cas. Il est évident que l'application $\theta : a \mapsto [a, x]$ est

un endomorphisme de A. Mieux, il commute avec toutes les conjugaisons de G, i.e.

$$[a, x]^g = [a^g, x] \text{ pour tous } a \in A, \quad g \in G,$$

car $x^g \equiv x \pmod{A}$ (en faisant intervenir les relations entre commutateurs établies dans le § 3).

a) Puisque $\operatorname{Ker} \theta < A$ et que A est min-irréductible par rapport à G, $\operatorname{Ker} \theta$ est fini ou, ce qui revient au même, l'intersection $X \cap A$ est finie. L'image A^θ est alors infinie, d'où, en vertu de la min-irréductibilité, $A = A^\theta = [A, x]$. Il est clair maintenant que pour tout $g \in G$ il existe un $a \in A$ tel que $[g, x] = [a, x]$, d'où $ga^{-1} \in X$ et donc $G = AX$.

b) Puisque $\operatorname{Ker} \theta < A$, le groupe $A/\operatorname{Ker} \theta \simeq A^\theta$ est sans torsion et A est max-irréductible par rapport à G, on a $\operatorname{Ker} \theta = 1$ ou, ce qui revient au même, $X \cap A = 1$. Ensuite, le groupe quotient A/A^θ est fini en vertu de la proposition 7.2.3 ; soit m son ordre. Le groupe G induit dans A/A^θ (par conjugaisons) un groupe d'automorphismes isomorphe à G/C, où $C = C_G(A/A^\theta)$, donc G/C est fini, lui aussi. Si $c \in C$, on a $[c, x]^m \in A^\theta = [A, x]$. Ensuite,

$$[c^m, x] \equiv [c, x]^m \pmod{[C, x, C]},$$

$$[C, x, C] \leqslant [A, C] \leqslant [A, x],$$

si bien que $[c^m, x] = [a, x]$ pour un certain $a \in A$. D'où $c^m a^{-1} \in X$, $c^m \in XA$. Il s'ensuit que le groupe quotient G/XA est périodique ; il ne reste qu'à montrer qu'il est de type fini.

Soient $a_1, \ldots, a_m$ les représentants des classes de A suivant le sous-groupe $[A, x]$. Pour tout $j = 1, \ldots, m$, choisissons dans G un élément g_j tel que $a_j = [g_j, x]$, et si un tel élément n'existe pas, posons $g_j = 1$. Pour tout $g \in G$ on a $[g, x] = a_i\,[b_i, x]$, en choisissant convenablement i et $b_i \in A$. Donc

$$[gb_i^{-1}, x] = a_i = [g_i, x],$$

d'où

$$gb_i^{-1}g_i^{-1} \in X, \quad g \in \operatorname{gr}(g_1, \ldots, g_m, X, A).$$

Il est clair maintenant que le groupe G/XA est de type fini. Le lemme est démontré.

24.2.2. Théorème (S.N. Tchernikov). *Tout groupe résoluble G dont les sous-groupes abéliens vérifient la condition minimale est un groupe de Tchernikov.*

(Remarquons qu'en réalité S.N. Tchernikov a démontré dès le début un théorème beaucoup plus fort (24.3.4) dont 24.2.2 est un cas particulier. Comme quoi un exposé logique ne tient pas toujours compte de la chronologie des événements.)

Démonstration. Raisonnons par récurrence sur le degré de résolubilité du groupe G. Comme nous l'avons signalé au commencement de ce n°, il suffit de montrer que si G vérifie la condition minimale pour ses sous-groupes abéliens et A est son sous-groupe normal abélien, le groupe quotient G/A vérifie à son tour la condition minimale pour ses sous-groupes abéliens. Remarquons à toute fin utile que la démonstration d'une proposition pareille pour le couple G, A se trouve grandement facilitée dans bien des cas si l'on décompose A en une matriochka G-permise,

$$1 = A_1 \leqslant A_2 \leqslant \ldots \leqslant A_{n+1} = A,$$

et si l'on considère ensuite le couple G, A_1, puis le couple G/A_1, A_2/A_1, etc.

Supposons d'abord que A soit fini et montrons que tout sous-groupe abélien B/A de G/A vérifie bien la condition minimale. Le groupe $B/C_B(A)$ est fini, lui aussi (parce qu'isomorphe à un sous-groupe de Aut A) et, bien sûr, $A \leqslant C_B(A)$. Admettons donc que $[A, B] = 1$, sans que A soit nécessairement fini. Choisissons dans B un sous-groupe normal abélien maximal quelconque M. Il est évident que $A \leqslant M$ et, puisque B est nilpotent, on a $M = C_B(M)$ (voir le théorème 16.2.6). Il est facile de voir que l'application

$$\tau : B/M \to \mathrm{Hom}\,(M/A, A)$$

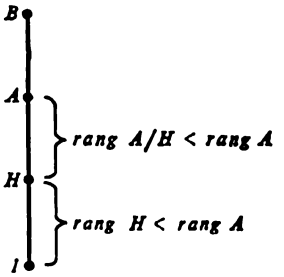
définie par la loi

$$(bM)^\tau : xA \mapsto [x, b]$$

est une injection (voir la définition de Hom dans l'exercice 5.1.6). Puisque B (et même G tout entier) est périodique et que M vérifie la condition minimale, il suffit de s'assurer que la partie périodique du groupe Hom $(M/A, A)$ est finie. D'après les résultats de l'exercice 24.1.8, on a $M/A = P \oplus Q$, où P est un groupe complet et Q un groupe fini ; il suffit donc de vérifier que tout élément périodique φ de Hom $(M/A, A)$ opère trivialement sur P, i.e. applique P dans 0. Or, il en est effectivement ainsi : si φ envoyait un élément quelconque $x \in P$ ailleurs que dans 0, l'homomorphisme $n\varphi$ (pour tout $n \geqslant 1$) appliquerait les éléments de l'ensemble $\frac{1}{n}x$ aussi ailleurs que dans 0.

Supposons maintenant que A soit infini. Décomposant A en une matriochka G-permise à sections primaires, finies ou complètes, nous remarquons qu'il suffit de prendre le cas où A est un p-groupe abélien complet. Montrons que dans ce cas tout sous-groupe abélien B/A de G/A vérifie aussi la condition minimale. La proposition étant triviale pour $A = 1$, procédons par récurrence sur le rang de A. Supposons d'abord que A soit min-réductible par rapport à B, i.e. contienne un sous-groupe H B-permis propre complet non trivial.

Puisque tout sous-groupe complet est facteur direct dans un groupe abélien (théorème 9.1.4) et que le rang d'un produit direct fini de p-groupes quasi cycliques est égal au nombre des facteurs, on obtient ce qui suit :



Remontant la matriochka $1 \leqslant H \leqslant A$, nous voyons que le rang du groupe B/A est fini. Soit maintenant A min-irréductible par rapport à B. On peut aussi admettre que $[A, B] \neq 1$, le cas contraire ayant été discuté plus haut. En vertu du lemme 24.2.1, cas a), B admet un sous-groupe X tel que

$$B = XA \quad \text{et} \quad |X \cap A| < \infty.$$

Conformément au cas que l'on vient d'examiner (A fini), le sous-groupe X vérifie la condition minimale, d'où il s'ensuit que B et B/A la vérifient, eux aussi. Le théorème est démontré.

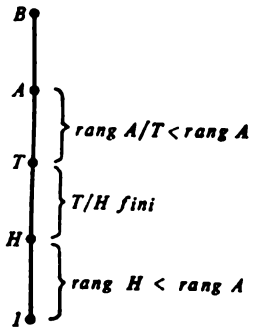
24.2.3. Théorème (A.I. Maltsev). *Tout groupe résoluble dont tous les sous-groupes abéliens vérifient la condition maximale est polycyclique.*

Démonstration. On suit le même plan. Supposons que G vérifie la condition maximale pour ses sous-groupes abéliens ; soit A son sous-groupe normal abélien ; on se propose de montrer que le groupe quotient G/A vérifie, lui aussi, la condition maximale pour ses sous-groupes abéliens.

Admettons d'abord, comme précédemment, que $[A, B] = 1$ (en particulier, le cas de A fini est couvert par cette conjecture). Soient M, τ les mêmes que précédemment. Puisque M/A et A sont des groupes abéliens de type fini, le groupe additif Hom $(M/A, A)$ est de type fini, lui aussi (voir l'exercice 8.1.8), ainsi que le groupe B/M plongé dans ce dernier. Par conséquent, B et B/A vérifient la condition maximale.

Passant au cas général, on peut dire que A est sans torsion, car sa partie périodique A_0 est finie et on peut donc monter au-dessus de A_0 en vertu de ce qui précède. Montrons comme précédemment que

tout sous-groupe abélien B/A de G/A vérifie la condition maximale. La proposition étant triviale pour $A = 1$, procédons par récurrence sur le rang de A. Supposons d'abord que A soit max-réductible par rapport à B, i.e. qu'il existe dans A un sous-groupe B-permis non trivial H admettant un groupe quotient non périodique A/H. Soit T/H partie périodique du groupe A/H. Puisque le rang de tout groupe abélien de type fini sans torsion se confond avec sa dimension et que les dimensions s'additionnent par passage au quotient (voir l'exercice 7.2.2), on obtient ce qui suit :



Remontant la matriochka $1 \leqslant H \leqslant T \leqslant A$, on remarque que le rang de B/A est fini. Soit maintenant A max-irréductible par rapport à B. On peut admettre aussi que $[A, B] \neq 1$ (le cas contraire ayant été discuté plus haut). En vertu du lemme 24.2.1, cas b), il existe un sous-groupe X tel que

$$|B : XA| < \infty \text{ et } X \cap \quad = 1.$$

Puisque le sous-groupe $X \simeq XA/A$ est abélien, il vérifie la condition maximale ; il en est de même, par suite, pour XA. Par conséquent, B et B/A vérifient à leur tour la condition maximale. Le théorème est démontré.

Il y a lieu de signaler à toute fin utile que les théorèmes 24.2.2 et 24.2.3 sont résumés par un théorème plus général :

24.2.4. Théorème. *Soit A un sous-groupe normal abélien du groupe G. Si G vérifie la condition minimale (resp. maximale) pour ses sous-groupes abéliens, le groupe quotient G/A vérifie, lui aussi, la condition minimale (resp. maximale) pour ses sous-groupes abéliens.*

24.2.5. Exercice. Un groupe résoluble dont tous les sous-groupes abéliens sont finis est fini lui-même.

24.3. Sur les groupes localement résolubles. Dans ce n°, le théorème 24.2.2 sur les groupes résolubles sera étendu aux groupes localement résolubles, acquérant ainsi un caractère aussi général que possible. Notons tout de suite que le théorème parallèle 24.2.3 ne se

prête pas à une généralisation pareille : on en discutera les raisons dans le paragraphe suivant, en décrivant un obstacle analogue pour les groupes de rang fini.

Commençons par un cas particulier :

24.3.1. Lemme. *Tout p-groupe localement fini G vérifiant la condition minimale pour ses sous-groupes abéliens est un groupe résoluble de Tchernikov.*

Démonstration. a) En vertu du théorème 24.2.2, il suffit de montrer que G est résoluble. Etant donné qu'un groupe non résoluble admet des sous-groupes dénombrables non résolubles, on peut admettre que G est dénombrable et non trivial.

b) Le centre $Z(G)$ de G est non trivial. En effet, étant dénombrable, G se laisse mettre sous la forme de la réunion d'une suite strictement croissante de sous-groupes finis $1 < G_1 < G_2 < \ldots$ Soit $Z_i = Z(G_i)$, $i = 1, 2, \ldots$ Puisque le centre d'un p-groupe fini est non trivial (voir l'exemple 17.1.1), aucun des Z_i n'est trivial. Ils engendrent un sous-groupe abélien

$$Z = \mathrm{gr}\,(Z_1, Z_2, \ldots)$$

qui vérifie donc la condition minimale. Compte tenu de la structure des groupes abéliens vérifiant la condition minimale (exercice 24.1.8), nous voyons que les éléments z de Z vérifiant la condition $z^p = 1$ forment un sous-groupe fini P. Puisque $P \leqslant G_i$ pour un certain i, on a $P \cap Z_i \geqslant P \cap Z_{i+1} \geqslant \ldots$, donc $P \cap Z_j = P \cap Z_{j+1} = \ldots$ pour un certain j. Il est clair que $1 < P \cap Z_j \leqslant Z(G)$.

c) Tous les hypercentres de G sont résolubles. Supposons au contraire qu'un α-ième hypercentre $\zeta_\alpha G$ de G soit non résoluble, α étant le premier ordinal possédant cette propriété. Il est clair que c'est un ordinal limite et qu'il est supérieur à zéro. Posons pour alléger l'écriture $L = \zeta_\alpha G$ et choisissons dans L un sous-groupe normal abélien maximal quelconque M. Il est évident que L est un ZA-groupe, d'où, conformément à l'exercice 22.1.7, $M = C_L(M)$. Soit A/M un sous-groupe normal abélien maximal dans L/M. En vertu du théorème 24.2.4, le groupe A/M vérifie la condition minimale. Il est évident que M vérifie aussi cette condition et se laisse représenter sous la forme de la réunion d'une suite strictement croissante de ses sous-groupes finis $M_1 < M_2 < \ldots$ normaux dans L. Puisque

$$C_A(M_1) \geqslant C_A(M_2) \geqslant \ldots,$$

l'on aura à partir d'un certain i

$$C_A(M_i) = C_A(M_{i+1}) = \ldots = C_A(M) = M.$$

Le groupe $A/M \simeq A/C_A(M_i)$ se plonge dans $\mathrm{Aut}\, M_i$, ce qui veut dire qu'il est fini. Donc, L/M (un ZA-groupe) est fini, lui aussi

(voir la dernière remarque de l'exercice 22.1.7). Par conséquent, L est résoluble.

d) Le groupe G est résoluble. En effet, si $\zeta_\beta G < G$, il ressort du théorème 24.2.4 que le groupe quotient $G/\zeta_\beta G$ vérifie la condition minimale pour ses sous-groupes abéliens (on ne doit pas oublier que $\zeta_\beta G$ est résoluble en vertu de c)). En vertu de b), le centre de ce groupe quotient est non trivial, d'où $\zeta_\beta G < \zeta_{\beta+1} G$. Ainsi donc, la suite d'hypercentres $\{\zeta_\beta G\}$ atteint G tout entier, donc, toujours en vertu de c), le groupe G est résoluble. Le lemme est démontré.

24.3.2. Lemme. *Soient G un groupe localement fini, p un nombre premier, $S = X/Y$ une section de G, et $S_1 < S_2 < \ldots$ une suite strictement croissante infinie de p-sous-groupes finis de S. Il existe alors dans X une suite strictement croissante de p-sous-groupes finis $P_1 < P_2 < \ldots$ tels que*

$$S_i = P_i Y/Y, \quad i = 1, 2, \ldots$$

Démonstration. Choisissons un représentant dans chaque classe suivant Y faisant partie d'une section (finie) S_i, et considérons le sous-groupe F_i engendré par ces représentants. Puisque G est localement fini, F_i est fini et l'on a de toute évidence $S_i = F_i Y/Y$. On peut admettre que $F_1 \leqslant F_2 \leqslant \ldots$ Choisissons un p-sous-groupe de Sylow P_i dans chaque F_i de telle sorte que $P_1 \leqslant P_2 \leqslant \ldots$ Puisque, dans les homomorphismes des groupes finis, l'image de tout sous-groupe de Sylow est encore un sous-groupe de Sylow (exercice 11.3.4) et que le passage au quotient de F_i par $F_i \cap Y$ donne un p-groupe (isomorphe à S_i), on obtient $P_i (F_i \cap Y) = F_i$. Il devient clair que $F_i Y = P_i Y$ et que $P_1 < P_2 < \ldots$

24.3.3. Lemme. *Soit G un groupe localement fini. S'il vérifie la condition minimale pour ses sous-groupes abéliens, il n'admet aucune section abélienne élémentaire infinie. Si tous les sous-groupes de Sylow sont finis dans G, il en est de même dans toutes les sections de G.*

Démonstration. Supposons que G vérifie la condition minimale pour ses sous-groupes abéliens et admet une section abélienne élémentaire dénombrable S. Soit $S_1 < S_2 < \ldots$ une suite strictement croissante de sous-groupes finis de S dont la réunion est égale à S, et soit $P_1 < P_2 < \ldots$ la suite de p-sous-groupes de G qui correspond à la suite précédente en vertu du lemme 24.3.2. Puisque le groupe $P = \bigcup P_i$ vérifie la condition minimale pour ses sous-groupes abéliens, P est un groupe de Tchernikov (lemme 24.3.1). Cela revient à dire que les rangs de tous les P_i sont bornés. Or, cela est impossible, car les rangs des S_i ne sont pas bornés. Quant à la seconde proposition du lemme, elle est immédiate en vertu du lemme 24.3.2.

24.3.4. Théorème (S.N. Tchernikov). *Tout groupe localement résoluble vérifiant la condition minimale pour ses sous-groupes abéliens est un groupe résoluble de Tchernikov.*

Démonstration. Soit G un groupe localement résoluble vérifiant la condition minimale pour ses sous-groupes abéliens. En vertu du théorème local de A.I. Maltsev 22.3.2, G admet une RI-matriochka. Soit $\mathcal{M}$ une RI-matriochka non subdivisible de G. Il est évident que chaque section S de $\mathcal{M}$ est un groupe abélien périodique Aut-simple, aussi S est-il un groupe abélien élémentaire (voir l'exercice 5.2.8). De plus, il est fini en vertu du lemme 24.3.3.

Soit R le sous-groupe engendré par tous les sous-groupes quasi cycliques dans G. Puisque R ne contient aucun sous-groupe d'indice fini (voir l'exercice 2.4.10), il stabilise $\mathcal{M}$, i.e. induit un groupe d'automorphismes unité dans chaque section S de $\mathcal{M}$. Il admet donc une matriochka centrale (voir l'exercice 22.1.5). Etant localement fini, R est localement nilpotent. En vertu de l'exercice 18.1.5 et du lemme 24.3.1, R est un groupe de Tchernikov; puisqu'il ne contient aucun sous-groupe propre d'indice fini, R est un groupe abélien.

Le groupe quotient G/R ne contient déjà aucun sous-groupe quasi cyclique. En effet, raisonnons par absurde et supposons qu'il existe un sous-groupe de ce type H/R, i.e. qu'il existe dans G des éléments $1 = a_1, a_2, \ldots$ tels que

$$H = \mathrm{gr}\,(a_1, a_2, \ldots)\cdot R$$

et

$$a_{i+1}^p \equiv a_i \pmod{R}, \quad i = 1, 2, \ldots$$

Le groupe H, opérant par conjugaisons dans R, induit des automorphismes dans R. S'il y avait dans R au moins un automorphisme non identique, on pourrait, en prenant l'élément de R déplacé par l'automorphisme en question et en ajoutant tous les éléments de même ordre de R, obtenir un ensemble fini M sur lequel H opère de façon non identique. Le sous-groupe H_0 de tous les éléments de H opérant sur M de façon identique contient R et est d'indice fini dans H. Puisque $H/H_0 \simeq (H/R)/(H_0/R)$ et que H/R ne contient aucun sous-groupe propre d'indice fini, il y a contradiction. Il s'ensuit que H commute avec R élément par élément. Ceci noté, remplaçons les éléments $1 = a_1, a_2, \ldots$ par des éléments $1 = b_1, b_2, \ldots$ tels que

$$b_i \equiv a_i \pmod{R}, \quad b_{i+1}^p = b_i, \quad i = 1, 2, \ldots.$$

En effet, supposons que les $b_1, \ldots, b_i$ soient déjà construits et que $a_{i+1}^p = b_i r_i$, $r_i \in R$. Choisissons dans R un élément x_{i+1} tel que $x_{i+1}^p = r_i$ et posons $b_{i+1} = a_{i+1}x_{i+1}^{-1}$. Il est clair que $b_{i+1} \equiv a_{i+1} \pmod{R}$ et $b_{i+1}^p = b_i$. Les éléments $b_1, b_2, \ldots$ ainsi cons-

truits engendrent évidemment dans G un sous-groupe quasi cyclique non inclus dans R, ce qui contredit le choix du sous-groupe R.

Puisque, en vertu de ce qui précède, le groupe G/R ne contient aucun sous-groupe quasi cyclique et vérifie la condition minimale pour ses sous-groupes abéliens (théorème 24.2.4), tous ses sous-groupes abéliens et tous ses sous-groupes de Sylow sont finis (voir l'exercice 24.1.8 et le lemme 24.3.1 respectivement). Montrons que G/R est fini lui-même.

Soit donc G un groupe localement résoluble dont tous les sous-groupes abéliens et tous les sous-groupes de Sylow sont finis. Il s'agit de montrer que G est lui-même un groupe fini. Puisque tout groupe infini contient des sous-groupes dénombrables, il suffit de montrer que G n'est pas dénombrable. Supposons au contraire que G soit dénombrable. Etant localement fini (voir l'exercice 24.2.5), G se laisse mettre sous la forme de la réunion d'une suite strictement croissante de sous-groupes finis $G_1 < G_2 < \ldots$

Puisque chaque G_n est fini et résoluble, il contient un p_n-sous-groupe normal abélien élémentaire A_n (voir l'exercice 19.1.7). Si, parmi les nombres premiers $p_1, p_2, \ldots$, on ne trouve qu'une quantité finie de p_n distincts, il est possible de construire une sous-suite particulière dans laquelle on peut admettre que tous les p_n coïncident avec un certain p. Soit

$$A = \mathrm{gr}\,(A_1, A_2, \ldots) = A_1 A_2 \ldots$$

Puisque les sous-groupes de Sylow dans G sont finis, A est fini. Or, on trouve alors parmi les sous-groupes $A_1, A_2, \ldots$ une infinité de A_n qui coïncident, i.e. G admet un sous-groupe normal abélien élémentaire fini K_1.

En vertu de l'exercice 24.2.5 et du lemme 24.3.3, tous les sous-groupes abéliens et tous les sous-groupes de Sylow dans le groupe localement résoluble G/K_1 sont encore finis. Reprenons notre raisonnement précédent en mettant G/K_1 à la place de G. S'il existe dans G/K_1 un sous-groupe normal abélien élémentaire fini K_2/K_1, nous répéterons le raisonnement pour G/K_2, et ainsi de suite. Finalement, ou bien nous construirons dans G une suite strictement croissante infinie de sous-groupes normaux finis $K_1 < K_2 < \ldots$, ou bien nous aboutirons à un groupe quotient G/K_i, pour lequel l'extraction des groupes A_n implique une suite de nombres premiers p_n contenant une infinité de termes distincts.

Plaçons-nous dans le premier cas et considérons le groupe $K = \bigcup K_i$. Pour tout p premier il n'admet qu'un nombre fini de sections K_{i+1}/K_i d'ordres divisibles par p (car les sous-groupes de Sylow de G sont finis), d'où il ressort que l'ensemble $\pi(K)$ de tous les diviseurs premiers des ordres des éléments de K est infini. Ensuite, pour tout $p \in \pi(K)$ l'ensemble des éléments d'ordre p dans K est fini, car tous les p-sous-groupes de Sylow de K sont contenus dans un

K_i. Soient $p_1 \in \pi(K)$, a_1 un élément d'ordre p_1 dans K, et $C_1 = C_K(a_1)$. Puisque

$$|K : C_1| = |a_1^K| < \infty$$

(voir le théorème 2.5.6), l'ensemble $\pi_1 = \pi(C_1)$ est infini, lui aussi. Choisissons dans π_1 un élément $p_2 \neq p_1$ et dans C_1 un élément a_2 d'ordre p_2. Puisque le sous-groupe

$$C_2 = C_K(a_1, a_2) = C_K(a_1) \cap C_K(a_2)$$

est d'indice fini dans K, l'ensemble $\pi_2 = \pi(C_2)$ est infini. Choisissons dans π_2 un élément $p_3 \neq p_1, p_2$ et dans C_2 un élément a_3 d'ordre p_3, etc. Nous obtiendrons par ce procédé des éléments $a_1, a_2, \ldots$ d'ordres respectifs $p_1, p_2, \ldots$, qui commutent deux à deux. Puisque ces éléments engendrent un sous-groupe infini, le premier cas est impossible.

Passant au second cas, supposons que la suite $p_1, p_2, \ldots$ contient une infinité de nombres distincts déjà pour G lui-même. On peut faire mieux et admettre que les $p_1, p_2, \ldots$ sont eux-mêmes tous distincts, sinon il suffirait d'éliminer les groupes G_n qui correspondent aux p_n répétés.

De la suite de groupes $A_1, A_2, \ldots$ on ne peut extraire aucune suite infinie de groupes cycliques. En effet, supposons au contraire qu'une sous-suite pareille $A_{k_1}, A_{k_2}, \ldots$ existe. Posons

$$B_j = \mathrm{gr}(A_{k_j}, A_{k_{j+1}}, \ldots), \quad j = 1, 2, \ldots$$

Puisque le groupe B_1 admet une matriochka normale $B_1 > B_2 > \ldots$ à sections cycliques, son commutant B_1' admet une matriochka centrale (voir l'exercice 22.1.6). Etant localement fini, le groupe B_1' est localement nilpotent et se décompose donc en produit direct de ses sous-groupes de Sylow (voir l'exercice 18.1.5). Or, ses sous-groupes de Sylow sont cycliques, i.e. B_1' est abélien. Ainsi donc, le groupe B_1 est résoluble et par suite, fini (voir l'exercice 24.2.5). Or, cela est en contradiction avec la définition même de B_1.

Ainsi donc, le nombre des groupes cycliques est au plus fini parmi les $A_1, A_2, \ldots$; on peut donc admettre qu'ils y sont absents. Puisque A_i et A_j sont des groupes abéliens élémentaires non cycliques des périodes différentes pour $i \neq j$, leur produit A_iA_j contient, d'après les résultats de l'exercice 6.1.6, un élément d'ordre p_ip_j; il s'ensuit que les groupes A_i, A_j admettent des éléments permutables a_i, a_j distincts de l'unité. Considérons l'ensemble des couples

$$(x_1, x_i), \text{ où } x_1 \in A_1, \quad x_i \in A_i, \quad x_1x_i = x_ix_1,$$

$i = 2, 3, \ldots$ Puisque le groupe A_1 est fini, il existe une infinité de couples

$$(b_1, x_{i_1}), \quad (b_1, x_{i_2}), \ldots$$

où le premier élément reste le même. Il existe donc dans A_1 un élément b_1 distinct de l'unité dont le centralisateur dans G contient un sous-groupe infini N_1 où b_1 n'intervient pas. Etant donné que N_1 vérifie les mêmes conditions que G, il existe dans N_1 un élément $b_2 \neq 1$ dont le centralisateur dans G contient un sous-groupe infini N_2 où b_2 n'intervient pas, et ainsi de suite. Il est évident que les $b_1, b_2, \ldots$ commutent deux à deux et engendrent un sous-groupe infini. Or, cela est impossible, car tous les sous-groupes abéliens de G sont finis. Le théorème est démontré.

On trouve dans [35] une théorie générale des groupes dont le système de sous-groupes possède des propriétés données. Cette théorie est développée depuis les années 40 par S.N. Tchernikov, un des fondateurs de la théorie des groupes contemporaine, et par ses disciples.

§ 25. La finitude du rang

25.1. Exemples. Considérons d'abord quelques groupes concrets intéressants et calculons la valeur numérique de leur rang ou au moins majorons-le.

25.1.1. Exemple. Soient p un nombre premier, m, n deux entiers naturels, $m \geqslant 2$. A l'exception du cas de $p = 2$, $k = 1$, tous les sous-groupes de congruence principaux

$$P_k = \mathrm{GL}_n(\mathbb{Z}_{p^m}, \quad p^k\mathbb{Z}_{p^m}), \quad k = 1, 2, \ldots,$$

du groupe $\mathrm{GL}_n(\mathbb{Z}_{p^m})$ sont de rang n^2 (on voit donc que le rang ne dépend ni de p, ni de m, ni de k).

En effet, de la description des groupes P_k donnée dans l'exercice 4.2.8, il ressort que P_{m-1} est un espace vectoriel de dimension n^2 sur un corps commutatif de p éléments; il suffit donc de montrer que pour $p > 2$ le rang du groupe P_1 est inférieur à n^2 et que pour $p = 2$ le rang de P_2 est inférieur à n^2. Les deux cas se traitant de façon analogue, nous nous bornerons à examiner le premier ($p > 2$).

Soit H un sous-groupe quelconque de P_1; il s'agit de montrer que H est engendré par n^2 éléments tout au plus. Soient φ_k les homomorphismes décrits dans l'exercice 4.2.8. Il est évident que

$$H^{\varphi_1} \leqslant (H \cap P_2)^{\varphi_2} \leqslant \ldots \leqslant (H \cap P_{m-1})^{\varphi_{m-1}} = H \cap P_{m-1}.$$

Choisissons dans l'espace vectoriel $H \cap P_{m-1}$ une base $a_1, \ldots, a_s$ telle que ses s_1 premiers éléments forment une base dans H^{φ_1}, ses s_2 premiers éléments forment une base dans $(H \cap P_2)^{\varphi_2}$, etc., $0 \leqslant s_1 \leqslant \leqslant \ldots \leqslant s \leqslant n^2$. Soit m_i le plus grand nombre pour lequel l'équation $x^{p^{m_i}} = a_i$ admette une solution dans H, par exemple b_i. Mon-

trons que H est engendré par les éléments $b_1, \ldots, b_s$. Supposons démontrée l'inclusion

$$H \cap P_{k+1} \leqslant \mathrm{gr}\,(b_1, \ldots, b_s);$$

soit $x \in H \cap P_k$. On a alors $x^{\varphi_k} = v\,(\ldots, a_i, \ldots)$, où v est un mot, $i \leqslant s_k$. Il est clair que

$$x = v\,(\ldots, b_i^{p^{m_i+k+1-m}}, \ldots)\,y, \quad y \in H \cap P_{k+1},$$

et que par suite $H \cap P_k \leqslant \mathrm{gr}\,(b_1, \ldots, b_s)$. On conclut alors par récurrence que H est inclus dans $\mathrm{gr}\,(b_1, \ldots, b_s)$ et se confond donc avec ce dernier groupe (l'inclusion inverse est évidente).

25.1.2. Exercice. Faire la démonstration pour $p = 2$, $k > 1$.

25.1.3. Exemple. Le rang d'un p-sous-groupe de Sylow de $\mathrm{GL}_n(\mathbb{Z}_{p^m})$ est inférieur à $\theta\,(n) = \frac{1}{2}\,(5n - 1)\,n$ (indépendant de m).

En effet, ce p-sous-groupe de Sylow P est décrit — à une conjugaison près — dans l'exercice 11.3.3. Soient les P_k les mêmes que précédemment (exercice 25.1.1). Considérons la suite de sous-groupes $P \geqslant P_1 \geqslant P_2$. Isomorphe à $\mathrm{UT}_n\,(p)$, le groupe quotient P/P_1 admet une matriochka normale à sections abéliennes de rangs $n - 1$, $n - 2, \ldots, 1$ (voir l'exemple 16.1.2). Le groupe quotient P_1/P_2 est soit trivial, soit abélien élémentaire de rang n^2. Enfin, P_2 est soit trivial, soit de rang n^2 conformément à l'exemple 25.1.1. De là et du théorème 4.1.7, il ressort que le rang de P est inférieur à $2n^2 + (n - 1) + (n - 2) + \ldots + 1 = \theta\,(n)$.

25.1.4. Exemple. De quelle façon la finitude du rang affecte-t-elle les propriétés locales du groupe, telles que la nilpotence locale? la résolubilité locale? Rappelons pour comparer que, par exemple, un groupe localement résoluble soumis à la condition d'être linéaire devient résoluble (exercice 21.1.6); par contre, il existe des groupes localement nilpotents linéaires qui ne sont pas nilpotents (exemples?). Nous allons montrer que la condition de finitude du rang ne fait pas nécessairement d'un groupe localement nilpotent un groupe nilpotent, ni d'un groupe localement résoluble un groupe résoluble.

Soit en effet n un entier naturel $\geqslant 3$. Considérons le produit direct de groupes de congruence:

$$G = \prod_p \mathrm{GL}_n\,(\mathbb{Z}_{m(p)}, \quad p\mathbb{Z}_{m(p)}),$$

dans lequel p parcourt tous les nombres premiers, $m\,(p) = p^{l(p)}$ et les $l\,(p)$ ne sont pas bornés dans leur ensemble. Puisque les facteurs de ce produit sont des p-groupes finis (voir la démonstration du

théorème 14.2.2), G est localement nilpotent. D'autre part, en vertu de la formule (9) du § 3

$$[t_{ik}(p^{2^l}),\quad t_{kj}(p^{2^l})] = t_{ij}(p^{2^{l+1}})$$

pour des i, j, k différents; il s'ensuit que les degrés de résolubilité des facteurs ne sont pas bornés dans leur ensemble et, par conséquent, G ne peut pas être résoluble. Ensuite, conformément à l'exercice 2.3.4 et à l'exemple 25.1.1, le rang de G est fini, à savoir: égal à n^2

25.1.5. E x e m p l e. Si A est un p-groupe abélien de rang fini r, tout p-sous-groupe Φ de son groupe des automorphismes est fini et le rang de Φ est inférieur à $\theta(r)$ (voir l'exemple 25.1.3).

Il est clair que l'exemple 25.1.3 n'intervient pas ici d'une façon accidentelle: il représente exactement le cas particulier de notre proposition où A est une somme directe de $r = n$ groupes cycliques de même ordre p^m. Il suffit de réduire la proposition générale au cas particulier, ce que nous ferons tout de suite.

Tout d'abord, en accord avec l'exercice 10.1.16 on a $A = B \oplus C$ (en notation additive), où B est un groupe fini et C une somme directe d'au plus r groupes quasi cycliques. Soient p^l le plus grand ordre des éléments de B, et A_0 le sous-groupe des éléments de A qui vérifient l'équation

$$p^{l'}x = 0, \text{ où } l' = \max(l, 2).$$

Il est évident que A_0 est fini et Aut-permis (et même End-permis) dans A. Montrons que si $\varphi \in \Phi$ et φ opère identiquement sur A_0, on a $\varphi = 1$. En effet, puisqu'on a $B \leqslant A_0$, l'automorphisme φ laisse invariants les éléments de B; il ne reste donc qu'à montrer que $\varphi|_C = 1$.

D'après les résultats de l'exercice 5.1.4, à l'automorphisme $\varphi|_C$ est associée une matrice α sur l'anneau des entiers p-adiques, telle que

$$\alpha \equiv \varepsilon \pmod{p^2},$$

car φ laisse invariantes toutes les solutions de l'équation $p^2x = 0$ (ε est la matrice unité). Si $\alpha \neq \varepsilon$, la matrice α doit être un élément d'ordre infini (voir l'indication à l'exercice 24.1.6), ce qui contredit la périodicité du groupe Φ. On a donc $\varphi = 1$.

Il résulte de ce qui précède que l'application associant à chaque automorphisme $\varphi \in \Phi$ sa restriction φ_0 au sous-groupe (Aut-permis fini) A_0 est un isomorphisme, i.e. $\Phi \simeq \Phi_0$, où Φ_0 est le groupe de tous les φ_0 de ce type. On peut donc admettre dès le début que A est f i n i.

Soit A une somme directe de groupes cycliques d'ordres $p^{m_1}, \ldots, p^{m_r}$, et soit $m = \max(m_1, \ldots, m_r)$. Plongeons A dans une somme « homogène »

$$A^* = (a_1) \oplus \ldots \oplus (a_r)$$

de termes de même ordre p^m, en posant

$$A = (p^{k_1}a_1) \oplus \ldots \oplus (p^{k_r}a_r),$$

où $k_i = m - m_i$, $i = 1, \ldots, r$. Pour chaque automorphisme φ de A on a

$$(p^{k_i}a_i)\varphi = \sum_j \alpha_{ij}(\varphi)(p^{k_j}a_j), \tag{1}$$

où $\alpha_{ij}(\varphi)$ sont des entiers convenablement choisis. On comprend que

$$\alpha_{ij}(\varphi) = \beta_{ij}(\varphi)\, p^{\max(k_i, k_j) - k_j},$$

où $\beta_{ij}(\varphi)$ sont aussi des entiers. Soit

$$\alpha^*_{ij}(\varphi) = \beta_{ij}(\varphi)\, p^{\max(k_i, k_j) - k_i}.$$

Un calcul matriciel bien simple montre que $\alpha^* = \delta^{-1}\alpha\delta$, où

$$\alpha = (\alpha_{ij}(\varphi)), \quad \alpha^* = (\alpha^*_{ij}(\varphi)), \quad \delta = \operatorname{diag}(p^{k_1}, \ldots, p^{k_r}).$$

Si maintenant $\varphi \in \Phi$ et $\varphi^{p^s} = 1$, on a $\alpha^{p^s} \equiv \varepsilon$ modulo le tapis d'idéaux

$$\begin{pmatrix} (p^{m_1}) & \ldots & (p^{m_r}) \\ \cdot & \cdot & \cdot \\ (p^{m_1}) & \ldots & (p^{m_r}) \end{pmatrix}.$$

Conjuguant cette relation par la matrice δ, nous remarquons qu'on a $(\alpha^*)^{p^s} \equiv \varepsilon$ modulo le tapis transposé

$$\begin{pmatrix} (p^{m_1}) & \ldots & (p^{m_1}) \\ \cdot & \cdot & \cdot \\ (p^{m_r}) & \ldots & (p^{m_r}) \end{pmatrix}.$$

Par conséquent, en élévant la matrice $(\alpha^*)^{p^s}$ à la puissance p^m, nous obtenons la matrice unité modulo p^m (cf. la démonstration du théorème 14.2.2). Cela revient à dire que α^* est une matrice d'ordre fini ; en particulier, elle est inversible. La matrice α^* définit un automorphisme φ^* du groupe « homogène » A^* par la formule

$$\alpha_i\varphi^* = \sum_j \alpha^*_{ij}(\varphi)\, a_j.$$

Il ressort de (1) que φ^* prolonge φ du sous-groupe A dans le groupe A^* tout entier. Il y a plus : si φ^*, ψ^* sont deux prolongements quel-

conques d'automorphismes φ, ψ de Φ, alors $\varphi^*\psi^*$ prolonge l'automorphisme $\varphi\psi$ et, pour les mêmes raisons que précédemment, est un p-élément. Il s'ensuit que l'ensemble Φ^* de tous les φ^* pris pour tous les $\varphi \in \Phi$ est un p-groupe d'automorphismes de A^*. En vertu de l'exemple 25.1.3, le rang du groupe Φ^* est inférieur à $\theta(r)$, aussi le rang de son image homomorphe Φ ne peut-il jamais être supérieur à ce nombre.

25.2. Passage des sous-groupes abéliens au groupe résoluble. Nous démontrerons, dans ce n°, un théorème d'importance capitale:

25.2.1. Théorème (M.I. Kargapolov). *Tout groupe résoluble dont les sous-groupes abéliens sont de rang fini est lui-même de rang fini.*

Compte tenu des considérations de récurrence exposées dans le paragraphe précédent à propos des théorèmes 24.2.2 et 24.2.3, nous démontrerons ce théorème sous la forme suivante:

25.2.2. Théorème. *Soit A un sous-groupe normal abélien d'un groupe G. Si les rangs des sous-groupes abéliens de G sont finis, ceux des sous-groupes abéliens du groupe quotient G/A le sont aussi.*

Commençons par démontrer quelques lemmes.

24.2.3. Lemme. *Soit A un sous-groupe normal abélien périodique de G. Si A est de rang fini et G/A contient un sous-groupe abélien libre de degré dénombrable, alors G contient de même un sous-groupe abélien libre de degré dénombrable.*

Démonstration. Soit $x_1A, x_2A, \ldots$ une base dénombrable dans un sous-groupe abélien libre de G/A, et soit $A_{ij} = \mathrm{gr}\,(x_i, x_j)$. En vertu du lemme 3.2.2, le commutant A'_{ij} du groupe A_{ij} est engendré par tous les éléments conjugués du commutateur $[x_i, x_j]$. Puisqu'ils sont tous contenus dans A et qu'un groupe abélien de rang fini et de période finie est fini (exercice 10.1.16), le commutant A'_{ij} est fini. Conformément à l'exercice 3.1.4, l'indice de son centralisateur dans A_{ij} doit être fini, si bien que A'_{ij} est centralisé par un élément $x_j^{n_{ij}}$, $n_{ij} > 0$. En particulier,

$$[x_i,\ x_j^{n_{ij}},\ x_j^{n_{ij}}] = 1,$$

d'où l'on déduit par récurrence sur m (compte tenu des relations entre commutateurs du § 3) que

$$[x_i,\ x_j^{n_{ij}m}] = [x_i,\ x_j^{n_{ij}}]^m, \quad m = 1,\ 2,\ \ldots$$

En particulier, pour $m = |A'_{ij}|$ on a $[x_i,\ x_j^{n_{ij}m}] = 1$. Posons

$$m_{ij} = n_{ij}\,|A'_{ij}|, \quad m_1 = 1 \text{ et } m_j = m_{1j}m_{2j}\ldots m_{j-1,\,j}$$

pour $j > 1$. Il est clair que gr $(x_1^{m_1}, x_2^{m_2}, \ldots)$ est un groupe abélien libre de degré dénombrable. Le lemme est démontré.

Passons maintenant aux groupes localement finis. Nous aurons besoin tout d'abord du lemme 24.3.1 auquel il est commode de donner l'énoncé suivant:

25.2.4. Lemme. *Un p-groupe localement fini dont tous les sous-groupes abéliens sont de rang fini est un groupe résoluble de Tchernikov.*

En effet, pour les p-groupes abéliens la condition de finitude du rang et la condition minimale coïncident (voir l'exercice 24.1.8).

25.2.5. Lemme. *Soient G un groupe localement fini dont tous les sous-groupes abéliens sont de rang fini, et p un nombre premier. Alors*

a) *les rangs des p-sous-groupes de Sylow de G sont finis et bornés dans leur ensemble,*

b) *les rangs des p-sections de G sont inférieurs à s_p, où s_p est le maximum des rangs des p-sous-groupes de Sylow de G,*

c) $s_p \leqslant \frac{1}{2}(5a_p + 1)\, a_p$, *où a_p est le maximum des rangs des p-sous-groupes abéliens de G.*

Démonstration. a) En vertu du lemme 25.2.4, les rangs de tous les p-sous-groupes de Sylow du groupe G sont finis; montrons qu'ils sont bornés dans leur ensemble. Supposons au contraire qu'il existe une suite de p-sous-groupes finis $P_1, P_2, \ldots$ de rangs illimités. Il existe alors une suite analogue pour laquelle chaque $Q_i = \mathrm{gr}\,(P_1, \ldots, P_i)$ est un p-groupe. En effet, si les $P_1, \ldots, P_i$ sont déjà choisis de telle façon que Q_i est un p-groupe, alors un sous-groupe conjugué de P_{i+1} est inclus dans le même p-sous-groupe de Sylow de Q_{i+1} que Q_i (en vertu du théorème de Sylow 11.1.1 appliqué au groupe fini Q_{i+1}). Remplaçons P_{i+1} par son conjugué; il s'ensuit que Q_{i+1} est lui aussi un p-groupe. Les $P_1, P_2, \ldots$ ainsi modifiés engendrent un p-sous-groupe. En vertu du lemme 25.2.4, son rang est fini, alors que ceux des sous-groupes $P_1, P_2, \ldots$ ne sont pas bornés: contradiction.

b) De toute évidence, il suffit de considérer les p-sections finies de G. Si L/M est une telle section, on a $L = XM$, où X est un sous-groupe fini. Soit P son p-sous-groupe de Sylow. Puisque l'homomorphisme $X \to XM/M$ envoie un p-sous-groupe de Sylow sur un p-sous-groupe de Sylow (voir l'exercice 11.3.4), on a

$$L = XM = PM, \tag{2}$$

d'où

$$\mathrm{rang}\, L/M \leqslant \mathrm{rang}\, P \leqslant s_p.$$

c) Soit P un p-sous-groupe de Sylow de rang s_p dans G. Puisque P est un groupe de Tchernikov (voir le lemme 25.2.4), il contient un sous-groupe normal abélien maximal M tel que P/M est un p-groupe fini. Par ailleurs, P est un ZA-groupe (voir la démonstration du lemme 24.3.1), donc, conformément à l'exercice 22.1.7, P/M admet une image isomorphe dans Aut M. Puisque le rang de M est inférieur à a_p, on a en vertu de l'exemple 25.1.5

$$\text{rang } P/M \leqslant \theta(a_p) = \frac{1}{2}(5a_p - 1)\, a_p.$$

Enfin, en vertu du théorème 4.1.7 on a

$$s_p \leqslant a_p + \theta(a_p) = \frac{1}{2}(5a_p + 1)\, a_p.$$

Le lemme est démontré.

25.2.6. Exercice. Dans les conditions du lemme 25.2.5, chaque p-section de G est un groupe de Tchernikov.

25.2.7. Lemme. *Soient G un groupe localement fini, A son sous-groupe normal, produit direct de ses sous-groupes de Sylow, et G/A un groupe abélien. Si les rangs des sous-groupes abéliens de G sont finis, G est lui-même de rang fini.*

Démonstration. a) On peut admettre que les sous-groupes de Sylow S_p/A de G/A sont finis pour tout p premier. En effet, tout S_p/A est un groupe de Tchernikov en vertu de l'exercice 25.2.6, si bien que son rang coïncide avec celui de la couche inférieure S_p^*/A, i.e. d'un sous-groupe maximal de période p. En montrant que le rang d'un groupe

$$G^* = \text{gr}\,(S_p^* \mid p \text{ premier})$$

est fini, nous démontrerons par là même la finitude des rangs de A et G^*/A, donc aussi de G/A (voir l'exercice 2.3.4) et finalement de G tout entier.

b) Les sous-groupes de Sylow sont conjugués dans G, ainsi que dans tout sous-groupe de G. En effet, tout p-sous-groupe de Sylow G_{pi} de G doit contenir l'unique p-sous-groupe de Sylow A_p de A. Puisque G_{pi}/A_p est fini, on a $G_{pi} = X_{pi}A_p$, où X_{pi} est un p-groupe fini (voir la démonstration de la formule (2) ci-dessus). Si Y_{pi}, Y_{pj} sont deux p-sous-groupes de Sylow du groupe fini gr (X_{pi}, X_{pj}) qui contiennent X_{pi}, X_{pj} respectivement, on a

$$G_{pi} = Y_{pi}A_p, \quad G_{pj} = Y_{pj}A_p,$$

donc, en vertu du théorème de Sylow 11.1.1, G_{pi} et G_{pj} sont conjugués dans G.

c) Il suffit de montrer que $G = TA$ pour un sous-groupe T qui se décompose en produit direct de ses sous-groupes de Sylow T_p.

En effet, si H_p est le sous-groupe abélien de plus grand rang dans un T_p, tous les H_p de ce type engendrent un sous-groupe abélien qui doit être de rang fini, par exemple de rang r. En vertu du lemme 25.2.5, c), le rang de chaque T_p reste inférieur à $\frac{1}{2}(5r+1)r$, d'où il ressort que le rang de T est fini (voir l'exercice 2.3.4). Pour les mêmes raisons, le rang de A et, par suite, de G tout entier est fini de même.

d) Construisons le sous-groupe T demandé.

Soit $p_1 = 2$, $p_2 = 3$, ... une suite de nombres premiers; soit S_i/A un p_i-sous-groupe de Sylow dans le groupe G/A. Considérons deux suites de sous-groupes

$$G = N_0 \geqslant N_1 \geqslant \ldots$$

et

$$P_1, P_2, \ldots,$$

où P_{i+1} est un p_{i+1}-sous-groupe de Sylow du groupe N_i,

$$N_{i+1} = N_{N_i}(P_{i+1}),$$

et montrons que $G = N_iA$ pour tout $i = 0, 1, 2, \ldots$ Le cas de $i = 0$ est trivial; passons donc de i à $i+1$. Il est évident que P_{i+1} est un p_{i+1}-sous-groupe de Sylow de l'intersection $N_i \cap S_{i+1}$ normale dans N_i; donc, en vertu du lemme généralisé de Frattini 17.1.9,

$$N_i = N_{i+1}(N_i \cap S_{i+1}).$$

Or,

$$N_i \cap S_{i+1} = P_{i+1}(N_i \cap A),$$

car la section $(N_i \cap S_{i+1})/(N_i \cap A)$ est un p-groupe fini (voir la déduction de la formule (2)). D'où

$$N_i = N_{i+1}(N_i \cap A)$$

et $G = N_iA = N_{i+1}A$ comme demandé.

D'après les résultats de l'exercice 25.2.6, le groupe P_i vérifie la condition minimale, si bien que la suite de ses sous-groupes

$$N_1 \cap P_i \geqslant N_2 \cap P_i \geqslant \ldots$$

est stationnaire, i.e. on obtient

$$N_{k(i)} \cap P_i = N_{k(i)+1} \cap P_i = \ldots$$

à partir d'un certain $k(i) \geqslant i$; désignons ces intersections par T_i. Si $k \geqslant k(i)$ et P est un p_i-sous-groupe quelconque de N_k, alors P normalise le sous-groupe P_i (car $N_k \leqslant N_{k(i)} \leqslant N_i$), d'où

$$P \leqslant N_k \cap P_i = T_i$$

et donc T_i est l'unique p_i-sous-groupe de Sylow du groupe N_k. Il s'ensuit que $[T_i, T_j] = 1$ pour $i \neq j$ et que par suite le sous-groupe

$$T = \mathrm{gr}\,(T_1, T_2, \ldots)$$

est produit direct de ses sous-groupes de Sylow $T_1, T_2, \ldots$

Le groupe T est celui qu'on cherche. En effet, il ne reste qu'à s'assurer que $G = TA$. Puisque $G = \mathrm{gr}\,(S_1, S_2, \ldots)\,A$, il suffit de démontrer l'égalité $S_i = T_iA$. Or,

$$S_i = (N_kA) \cap S_i = (N_k \cap S_i)\,A,$$

et si $k \geqslant k\,(i)$, on obtient

$$N_k \cap S_i = T_i\,(N_k \cap A)$$

(voir la déduction de la formule (2)). On a donc bien $S_i = T_iA$. Le lemme est démontré.

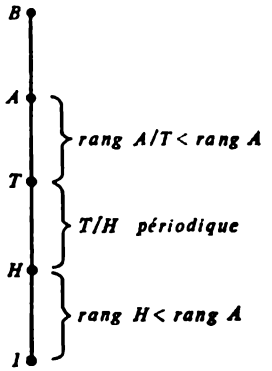
Démonstration du théorème 25.2.2. Il suffit évidemment d'examiner les deux cas extrêmes où A est un sous-groupe périodique ou un sous-groupe sans torsion, car dans le cas général on peut remonter la matriochka $1 \leqslant A_0 \leqslant A$, où A_0 est la partie périodique du groupe A.

Supposons d'abord que A soit périodique, et montrons que les rangs des sous-groupes abéliens du groupe G/A sont finis. Supposons au contraire que G/A admette un sous-groupe abélien B/A de rang infini. En vertu du lemme 25.2.7, sa partie périodique B_0/A doit être de rang fini, si bien que le groupe sans torsion B/B_0 doit être de rang infini. Alors B/B_0 est aussi de dimension infinie sur $\mathbb{Z}$ (sinon il serait plongé dans la somme directe finie $\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}$ dont le rang est fini) et contient donc un sous-groupe abélien libre de degré dénombrable. En vertu du lemme 25.2.3 appliqué successivement aux couples B/A, B_0/A et B, A, le groupe B lui-même doit contenir un tel sous-groupe. Or, cela contredit la finitude des rangs des sous-groupes abéliens de G.

Plaçons-nous dans le second cas où A est sans torsion. Montrons que là encore, tout sous-groupe abélien B/A du groupe G/A est de rang fini. Nous adopterons le même schéma et les mêmes notations que pour les théorèmes 24.2.2 et 24.2.3 ci-dessus (voir page 213). Si $[A, B] = 1$, il suffit de s'assurer, conformément au schéma retenu, que le groupe $\mathrm{Hom}\,(M/A, A)$ est de rang fini. Puisque M/A et A sont deux groupes abéliens de rang fini et que A est sans torsion, le groupe $\mathrm{Hom}\,(M/A, A)$ est isomorphe à un sous-groupe du groupe additif des matrices (rectangulaires) sur le corps $\mathbb{Q}$, i.e. il est de rang fini.

Dans le cas général, procédons par récurrence sur le rang du groupe A (pour $A = 1$ la proposition est triviale). Supposons d'abord que A soit max-réductible par rapport à B, i.e. qu'il contienne un sous-

groupe B-permis non trivial H de groupe quotient apériodique A/H. Soit T/H la partie périodique de A/H. Puisque le rang d'un groupe abélien sans torsion de rang fini coïncide avec sa dimension et que les dimensions s'additionnent par passage au quotient (voir l'exercice 7.2.2), on obtient ce qui suit:



En remontant la matriochka $1 \leqslant H \leqslant T \leqslant A$, nous voyons que le groupe B/A est de rang fini. Supposons maintenant que A soit max-irréductible par rapport à B. On peut admettre ensuite que $[A, B] \neq \neq 1$, car le cas contraire vient d'être discuté. Alors, en vertu du lemme 24.2.1, b), il existe un sous-groupe X tel que

$$|B : XA| < \infty \text{ et } X \cap A = 1.$$

Etant abélien, le sous-groupe $X \simeq XA/A$ est de rang fini, de même que les sous-groupes XA et B. Or, le sous-groupe B/A doit alors être de rang fini. Le théorème est démontré.

25.3. Sur les groupes localement résolubles. Comme nous l'avons déjà noté au commencement du n° 24.3, ni le théorème 24.2.3 ni le théorème 25.2.1 ne s'appliquent aux groupes localement résolubles, à la différence du théorème 24.2.2; nous le montrerons au moyen d'un exemple.

25.3.1. Exemple (Iou.I. Merzliakov). Il existe des groupes localement polycycliques sans torsion dont toutes les sections abéliennes sont de rang fini, mais les rangs des sous-groupes abéliens ne sont déjà pas bornés dans leur ensemble.

Pour construire de tels groupes, introduisons la notion de $\varkappa$-déformation. Nous considérerons des triplets de la forme (G, A, α), où G est un groupe, A son sous-groupe normal d'indice fini, qui est un groupe abélien libre de degré strictement positif fini (si bien que, dans le cas examiné, le degré de liberté coïncide avec le rang du

groupe), et α une base donnée dans A. Soit $\varkappa$ une suite finie d'entiers naturels premiers entre eux deux à deux ; la longueur de $\varkappa$ coïncide avec le rang de A ; k est le produit des nombres dans $\varkappa$. Désignons par $A^{\varkappa}$ le sous-groupe engendré par les éléments de α élevés à des puissances correspondantes de $\varkappa$, et par A^k le sous-groupe des puissances k-ièmes des éléments de A.

Soit Φ_k un polynôme circulaire d'ordre k,

$$\Phi_k(x) = x^n - c_1 x^{n-1} - \ldots - c_n.$$

Ici $n = \varphi(k)$, où φ est la fonction d'Euler. La matrice

$$\zeta_k = \begin{pmatrix} c_1 & c_2 & c_3 & \ldots & c_{n-1} & c_n \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & & \ddots & & \\ & & & & 0 & \\ & & & & 1 & 0 \end{pmatrix}$$

admet Φ_k comme polynôme caractéristique et engendre donc dans le groupe $\mathrm{GL}_n(\mathbb{Z})$ un sous-groupe cyclique d'ordre k.

Puisque $A/A^{\varkappa}$ est aussi un groupe cyclique d'ordre k, il admet une représentation fidèle par des puissances de la matrice ζ_k. Soit σ la composée de cette représentation et de l'homomorphisme canonique $A \to A/A^{\varkappa}$. Puisque l'indice $m = |G : A|$ est fini, la représentation $\sigma : A \to \mathrm{GL}_n(\mathbb{Z})$ induit la représentation $\bar{\sigma} : G \to \mathrm{GL}_{mn}(\mathbb{Z})$ d'après la loi suivante (voir la fin du n° 17.2) : on prend des représentants quelconques $u_1, \ldots, u_m$ dans les classes de G suivant A et on pose $g^{\bar{\sigma}} = ((u_i^{-1} g u_j)^{\sigma})$ pour $g \in G$; ici $x^{\sigma} = 0$ pour $x \notin A$.

Prenons maintenant un groupe abélien libre $B \simeq \mathbb{Z}^{mn}$ et admettons que $\bar{\sigma} : G \to \mathrm{Aut}\, B$. Soit $G^* = GB$ l'extension de B par le groupe G qui opère sur B conformément à $\bar{\sigma}$. Il est évident que le sous-groupe $A^* = A^k B$ est normal et d'indice fini dans G^* et est un groupe abélien libre de rang fini. Choisissons dans A^* une base α^* qui commence par les puissances k-ièmes des éléments correspondants de α. Le triplet (G^*, A^*, α^*) s'appelle *$\varkappa$-déformation* du triplet (G, A, α) et se note symboliquement par

$$(G, A, \alpha) \overset{\varkappa}{\rightsquigarrow} (G^*, A^*, \alpha^*). \tag{3}$$

25.3.2. Exercice. Montrer que si $a \in A$ et $a^g \notin A^{\varkappa}$ pour tout $g \in G$, on a $C_B(a) = 1$.

25.3.3. Lemme. *Si un entier naturel composé k se divise par un nombre premier mais ne se divise pas par son carré, on a* $\det(1 - \zeta_k) = 1$.

Démonstration. Ajoutons à la première colonne de la matrice $1 - \zeta_k$ ses autres colonnes et développons le déterminant de la matrice obtenue suivant sa première colonne ; nous voyons que $\det(1 - \zeta_k) = \Phi_k(1)$ (pour k quelconque). Appliquons maintenant la formule

$$x^k - 1 = \prod_{d \mid k} \Phi_d(x)$$

(voir par exemple [38]). Soit $k = pl$, où p est un nombre premier qui ne divise pas l. Alors

$$x^k - 1 = (x^l - 1) \cdot \prod_{d \mid l} \Phi_{pd}(x).$$

Dans le cas particulier où l est premier, on a

$$x^{l(p-1)} + x^{l(p-2)} + \ldots + x^l + 1 = \Phi_p(x)\,\Phi_k(x).$$

Posant ici $x = 1$, on obtient $\Phi_k(1) = 1$. Dans le cas général le raisonnement reste le même mais on procède par récurrence sur le nombre des diviseurs de l.

25.3.4. Lemme. *Soit k un entier naturel « square-free »* (voir page 156), *et t un entier naturel quelconque. La matrice ζ_k^t est conjuguée dans le groupe $\mathrm{GL}_{\varphi(k)}(\mathbb{C})$ avec le produit tensoriel $\zeta_{k/d} \otimes 1_{\varphi(d)}$, où $d = (k, t)$, 1_m la matrice unité d'ordre m. Si k/d est un nombre composé, on a* $\det(1 - \zeta_k^t) = 1$.

Démonstration. Tout d'abord

$$\zeta_k \sim \mathrm{diag}\,(\varepsilon_1, \ldots, \varepsilon_{\varphi(k)}),$$

où $\sim$ symbolise la conjugaison dans $\mathrm{GL}_{\varphi(k)}(\mathbb{C})$ et la diagonale réunit toutes les racines primitives k-ièmes de 1. Il est clair que pour $d = 1$ on a $\zeta_k^t \sim \zeta_k$. Soient maintenant $d > 1$ et $k = dk_1$, $t = dt_1$. On voit sans peine que

$$\zeta_k^d \sim \zeta_{k_1} \otimes 1_{\varphi(d)}.$$

Elevant les deux membres de cette relation à la t_1-ième puissance et tenant compte de la remarque précédente, on obtient la première proposition demandée. La seconde résulte immédiatement de la première en vertu du lemme 25.3.3.

Construisons à présent les groupes dont il a été question dans l'exemple 25.3.1.

a) Construction des groupes demandés. Tout d'abord, faisons la suite $\nu_1, \nu_2, \ldots$ de toutes les suites d'entiers, stationnaires sur 0. Soient G_1 un groupe polycyclique, presque abélien, sans torsion, A_1 son sous-groupe abélien libre d'indice fini, $\mathfrak{a}_1$ une base dans A_1.

Au départ du triplet $(G_1, A_1, \mathfrak{a}_1)$, construisons la suite des déformations

$$(G_1, A_1, \mathfrak{a}_1) \overset{\varkappa_1}{\sim\!\!\rightarrow} \ldots \sim\!\!\rightarrow (G_n, A_n, \mathfrak{a}_n) \overset{\varkappa_n}{\sim\!\!\rightarrow} \ldots$$

et passons à sa « limite ». Supposons en effet qu'un triplet $(G_n, A_n, \mathfrak{a}_n)$ soit déjà construit; soit $\mathfrak{a}_n^{\nu_i}$ le produit des éléments de $\mathfrak{a}_n$ élevés à des puissances correspondantes de ν_i (les composantes indiciées par des nombres plus grands que la longueur de $\mathfrak{a}_n$ ne sont pas utilisées). On comprend aisément que l'ensemble des éléments

$$(\mathfrak{a}_n^{\nu_i})^g, \quad g \in G_n, \quad i = 1, 2, \ldots, n, \tag{4}$$

est fini. Choisissons comme $\varkappa_n$ une suite finie de nombres « squarefree » premiers entre eux deux à deux, de telle façon que le groupe $A_n^{\varkappa_n}$ ne contienne ni éléments de (4) distincts de l'unité, ni leurs puissances d'exposant premier (pour que cette condition soit vérifiée, il suffit de demander par exemple que tous les nombres de $\varkappa_n$ soient composés et que leurs diviseurs premiers soient plus grands que les modules des coordonnées des éléments de (4) dans la base $\mathfrak{a}_n$). La construction d'un $(n+1)$-ième triplet s'opère maintenant à partir de la définition de la $\varkappa_n$-déformation, i.e. du triplet composé de

$$G_{n+1} = G_n B_n, \quad A_{n+1} = A_n^{k_n} B_n \tag{5}$$

et d'une base quelconque $\mathfrak{a}_{n+1}$ de A_{n+1} commencée par les puissances k_n-ièmes des éléments correspondants de $\mathfrak{a}_n$. Ici k_n, B_n ont le même sens que k et B dans la définition de la déformation (3).

Soit G_∞ la *déformation limite* du triplet $(G_1, A_1, \mathfrak{a}_1)$ par rapport à la suite des séquences $\varkappa_1, \varkappa_2, \ldots$, i.e. la réunion de la suite des groupes emboîtés $G_1 \leqslant G_2 \leqslant \ldots$ Nous allons montrer que G_∞ est le groupe cherché. En effet, compte tenu de (5), on s'assure facilement par récurrence sur n que tous les G_n sont des groupes polycycliques, sans torsion, de rangs finis. Ainsi donc, G_∞ est un groupe localement polycyclique sans torsion et contient des sous-groupes abéliens A_n dont les rangs croissent à l'infini. Il reste à vérifier que les rangs des sections abéliennes de G_∞ sont finis.

b) Pour tout élément $h \neq 1$ de G_∞ il existe un entier naturel $n(h)$ tel que pour tout $n \geqslant n(h)$ on trouve un élément $a_n \in \mathrm{gr}(h) \cap \cap A_n$ dont aucune puissance d'exposant premier ne figure dans les sous-groupes $(A_n^{\varkappa_n})^g$, $g \in G_n$. Plus exactement, si $h \in G_s$ et $h^{|G_s : A_s|} = \mathfrak{a}_s^{\nu_t}$ et si ν_t présente des zéros dans toutes les positions à partir de la $(|\mathfrak{a}_s| + 1)$-ième, on peut poser $n(h) = \max(s, t)$. En effet, soit $n \geqslant s, t$ et

$$a_n = h^{|G_s : A_s| \cdot k_s h_{s+1} \cdots k_{n-1}}.$$

Il est évident que $a_n = \alpha_n^{\nu_t} \in A_n$. D'autre part, puisque $t \leqslant n$, on a par construction de $\varkappa_n$ pour tout p premier

$$a_n^p = (\alpha_n^{\nu_t})^p \notin (A_n^{\varkappa_n})^g, \quad g \in G_n.$$

c) Passons à la démonstration proprement dite de la finitude des rangs des sections abéliennes de G_∞. Soient H un sous-groupe non trivial de G_∞, et H' son commutant. Il suffit de montrer que

$$\text{rang } H/H' \leqslant \text{rang } G_{n(H)},$$

où $n(H)$ est min $n(h)$ pour tous les $h \in H$, $h \neq 1$. Soit $n(H) = l$. Il suffit de montrer que le rang de tout sous-groupe de type fini dans H/H' est inférieur à celui de G_l ; sans diminuer la généralité, on peut donc admettre que H est lui-même de type fini et contient toujours un h_0 tel que $n(h_0) = l$. En particulier, $H \leqslant G_s$ pour un assez grand $s \geqslant 2$.

Puisque $G_s = G_l B_l B_{l+1} \ldots B_{s-1}$, le groupe G_s admet une matriochka normale finie

$$G_s = D_{l-1} > D_l > \ldots > D_s = 1,$$

où

$$D_n = B_n B_{n+1} \ldots B_{s-1}, \quad n = l, l+1, \ldots, s-1.$$

Cette matriochka induit dans H la matriochka

$$H = H_{l-1} \geqslant H_l \geqslant \ldots \geqslant H_s = 1, \text{ où } H_n = H \cap D_n,$$

et dans H/H' la matriochka

$$H/H' = \bar{H}_{l-1} \geqslant \bar{H}_l \geqslant \ldots \geqslant \bar{H}_s = 1, \text{ où } \bar{H}_n = H_n H'/H'.$$

Nous montrerons qu'on a en effet $\bar{H}_n/\bar{H}_{n+1} = 1$ pour $n = l, l+1, \ldots$ $\ldots, s-1$, i.e. que $\bar{H}_l = 1$ et $H/H' \simeq \bar{H}_{l-1}/\bar{H}_l$. Puisque $\bar{H}_{l-1}/\bar{H}_l$ est une section de $D_{l-1}/D_l \simeq G_l$, on obtient la majoration cherchée : rang $H/H' \leqslant$ rang G_l.

d) Soit donc $l \leqslant n < s$. Appliquant deux fois le théorème 4.2.4, on obtient

$$\begin{aligned}\bar{H}_n/\bar{H}_{n+1} &\simeq H_n H'/H_{n+1} H' \simeq H_n/H_{n+1}(H_n \cap H') = \\ &= (H \cap D_n)/(H' \cap D_n)(H \cap D_{n+1}) \simeq \\ &\simeq (H \cap D_n) D_{n+1}/(H' \cap D_n) D_{n+1} \simeq (H \cap D_n)^{\pi_n}/(H' \cap D_n)^{\pi_n},\end{aligned}$$

où π_n est la projection naturelle $D_n \to B_n$. Pour alléger l'écriture, introduisons les notations

$$L = (H \cap D_n)^{\pi_n}, \quad M = (H' \cap D_n)^{\pi_n}.$$

Il reste à montrer que $L = M$. Cette proposition étant immédiate pour $L = 1$, supposons que $L \neq 1$.

Soient $b \in L$, $b = h^{\pi_n}$, $h \in H \cap D_n$, i.e.

$$h \equiv b \pmod{D_{n+1}}, \quad b \in B_n.$$

Puisque $n(h_0) = l$ (voir le commencement de c)), il existe un élément $h_n \in \mathrm{gr}(h_0) \cap A_n$ tel que

$$h_n^p \notin (A_n^{\varkappa_n})^g$$

pour aucun p premier et aucun $g \in G_n$.

Remarquons que

$$(h_n^{-1}hh_n)^{-1}h = [h_n, h] \in H' \cap D_n \tag{6}$$

et

$$h_n^{-1}hh_n \equiv h_n^{-1}bh_n \pmod{D_{n+1}}.$$

Si $u_1, \ldots, u_m$ sont les représentants des classes de G_n suivant A_n, on a par construction de G_{n+1}

$$h_n^{-1}bh_n = b\hat{h}_n,$$

où l'élément b est écrit par une ligne de $\mathbb{Z}^{m \cdot \varphi(k_n)}$, la transformation linéaire $\hat{h}_n$ par la matrice

$$\mathrm{diag}\,((u_1^{-1}h_nu_1)^\sigma, \ldots, (u_m^{-1}h_nu_m)^\sigma)$$

et σ est la composée de l'homomorphisme canonique $A_n \to A_n/A_n^{\varkappa_n}$ et de l'isomorphisme subséquent sur le groupe (ζ_{k_n}). En vertu de (6)

$$[h_n, h] \equiv b\,(1 - \hat{h}_n) \pmod{D_{n+1}}. \tag{7}$$

En vertu du lemme 25.3.4, les déterminants des blocs $1 - (u_i^{-1}h_nu_i)^\sigma$ sont égaux à 1, d'où

$$\det(1 - \hat{h}_n) = 1.$$

En vertu du théorème 8.1.1 les groupes abéliens libres B_n, L admettent des bases compatibles

$$b_1, \ldots, b_r, b_{r+1}, \ldots, b_t, \tag{8}$$

$$m_1b_1, \ldots, m_rb_r, \tag{9}$$

où m_j sont des entiers non nuls. Puisque L est $\hat{h}_n$-permis, la transformation $1 - \hat{h}_n$ fait passer la base (9) à sa $\mathbb{Z}$-enveloppe linéaire et, par suite, fait revenir le groupe $L^* = \mathrm{gr}(b_1, \ldots, b_r)$ à lui-même. Nous voyons que cette transformation s'écrit dans la base (8) par une matrice entière à moitié désintégrée, donc

$$\det(1 - \hat{h}_n)|_L = \det(1 - \hat{h}_n)|_{L^*} = \pm 1.$$

Cela signifie que

$$L\,(1 - \hat{h}_n) = L.$$

De là et des relations (6), (7) il découle que $L = M$, ce qui achève la démonstration.

Remarquons que les groupes G_∞ possèdent aussi d'autres propriétés intéressantes:

25.3.5. Proposition. *Chacun des groupes G_∞ est localement résoluble mais ne possède pas la propriété RN^*, car chaque RN^*-sous-groupe (en particulier, chaque sous-groupe abélien) de G_∞ est contenu dans un G_n.*

Démonstration. a) Les normalisateurs et les centralisateurs dans G_∞. Montrons tout d'abord que

$$N_{G_{n+1}}(M) = N_{G_n}(M)\, C_{B_n}(M) \quad \text{pour } M \leqslant G_n. \tag{10}$$

En effet, soient des $g \in G_n$, $b \in B_n$ tels que $M^{gb} = M$. Puisque $[M, b^{-1}] \leqslant B_n$ et que d'autre part

$$[M, b^{-1}] \leqslant M^{-1}M^{b-1} = M^{-1}M^g \leqslant G_n,$$

on a $[M, b^{-1}] = 1$. D'où $b \in C_{B_n}(M)$, $g \in N_{G_n}(M)$ comme demandé.

Ensuite, conformément à l'exercice 25.3.2 et par construction de $\varkappa_n$, on a

$$C_{B_n}(\mathfrak{a}_n^{\nu_i}) = 1 \quad \text{pour } \mathfrak{a}_n^{\nu_i} \neq 1, \quad i \leqslant n. \tag{11}$$

b) Soit H un sous-groupe non trivial de G_∞, traversé par la suite sous-normale transfinie croissante

$$H = H_0 < H_1 < \ldots < H_\alpha < \ldots < H_\gamma,$$

i.e. $H_\alpha \lhd H_{\alpha+1}$ pour tous les ordinaux transfinis $\alpha < \gamma$ et $H_\alpha = \bigcup_{\beta<\alpha} H_\beta$ pour les ordinaux limites $\alpha \leqslant \gamma$. Si H est contenu dans un G_s, il existe un $n = n_H$ tel que $H_\gamma \leqslant G_n$.

En effet, soit $a \neq 1$ un élément de l'intersection $H \cap A_s$. Supposons que a admette dans la base $\mathfrak{a}_s$ des coordonnées $u_1, \ldots, u_r$ et que la suite $\nu = (u_1, \ldots, u_r, 0, \ldots)$ soit indiciée par t, i.e. $\nu = \nu_t$. Montrons que $n = \max(s, t)$ est le nombre cherché, i.e. $H_\gamma \leqslant G_n$. Supposons démontré que $H_\beta \leqslant G_n$ pour tous les $\beta < \alpha \leqslant \gamma$ et montrons que $H_\alpha \leqslant G_n$. Cela est évident pour α limite; soit donc α un ordinal transfini non limite. Il suffit de vérifier que

$$N_{G_{l+1}}(H_{\alpha-1}) = N_{G_l}(H_{\alpha-1}) \quad \text{pour } l \geqslant n,$$

ou, compte tenu de (10), que

$$C_{B_l}(H_{\alpha-1}) = 1 \text{ pour } l \geqslant n. \tag{12}$$

Or,

$$C_{B_l}(H_{\alpha-1}) \leqslant C_{B_l}(a) \leqslant C_{B_l}(a^{k_s \cdots k_{l-1}}). \tag{13}$$

En vertu du choix des bases données on a $a^{k_s \cdots k_{l-1}} = \alpha_l^{\gamma}$, si bien que (13) et (11) donnent lieu à (12).

La proposition 25.3.5 est complètement démontrée.

Ces exemples n'arrivent cependant pas à dissiper le doute ; pourquoi, des trois théorèmes 24.2.2, 24.2.3 et 25.2.1 parallèles d'après leur énoncé et le schéma de la démonstration, le premier se laisse généraliser pour les groupes localement finis et les deux autres non ? Le doute disparaît quand on considère l'important théorème suivant démontré par Iou.M. Gortchakov (*DAN SSSR*, 1964, 156, n° 1, p. 17-20) : *tout groupe périodique, localement résoluble dont les sous-groupes abéliens sont de rangs finis est lui-même de rang fini.* Ainsi donc, le parallélisme — et la paix dans l'âme — se rétablissent très facilement : chacun des trois théorèmes en question a lieu pour les groupes p é r i o d i q u e s, localement résolubles (nous laissons au lecteur le soin de discuter le dernier cas (facile) du théorème 24.2.3), et aucun des théorèmes n'a lieu pour les groupes sans torsion. On peut bien sûr répliquer que la famille des groupes vérifiant la condition minimale pour leurs sous-groupes abéliens ne contient que des groupes périodiques et ne contient aucun groupe sans torsion, ni même un groupe mixte : en effet, telles sont les mœurs austères de cette famille, découlant de sa définition même.

APPENDICE

QUELQUES RAPPELS D'ALGÈBRE, DE LOGIQUE ET DE THÉORIE DES NOMBRES

§ 26. Sur les algèbres nilpotentes

La relation entre la nilpotence d'un groupe et celle d'un anneau, mentionnée rapidement dans le texte, joue en réalité un rôle de premier plan, enrichissant tant la théorie des groupes que la théorie des anneaux. Nous donnons ici quelques notions sur les algèbres nilpotentes, nécessaires à l'étude des groupes engéliens (n° 18.3). Dans le premier n° nous établirons les définitions principales et nous verrons ce que devient la nilpotence lorsqu'on passe canoniquement de l'algèbre associative à l'algèbre de Lie et inversement. Le deuxième n° sera consacré à la construction de nil-algèbres non nilpotentes.

26.1. Nilpotence d'une algèbre associative et d'une algèbre de Lie. Soient k un corps commutatif et A un anneau (on ne demande ni que soit commutatif, ni que la multiplication dans A soit associative). L'anneau A est appelé *algèbre* (*linéaire*) *sur* k si pour tous $\alpha \in k$, $a \in A$ il existe un élément $\alpha a \in A$ et si cette « multiplication par un scalaire » est liée aux opérations dans k et A par les relations suivantes:

$$\begin{aligned}(\alpha + \beta)\, a &= \alpha a + \beta a,\\ (\alpha\beta)\, a &= \alpha\, (\beta a),\\ 1a &= a,\\ \alpha\, (a + b) &= \alpha a + \alpha b,\\ \alpha\, (ab) &= (\alpha a)\, b = a\, (\alpha b).\end{aligned}$$

Ici α, β sont deux éléments quelconques dans k, 1 l'unité du corps k, a, b deux éléments quelconques dans A. On dit que l'algèbre A est *associative* si

$$(ab)\, c = a\, (bc) \text{ pour tous } a,\ b,\ c \in A.$$

On dit que A est une *algèbre de Lie* si

$$ab + ba = 0,$$

$$(ab)\,c + (bc)\,a + (ca)\,b = 0$$

pour tous $a, b, c \in A$.

Le lecteur n'aura aucune peine à saisir l'importance de l'associativité. Quant aux algèbres de Lie, elles peuvent sembler de prime abord un peu artificielles. Or, en réalité elles sont tout aussi naturelles que les associatives : chaque algèbre associative admet une associée, à savoir : une algèbre de Lie qui se déduit par un procédé canonique. Soit A l'algèbre associative. Si a, b sont ses éléments, l'élément $(a, b) = ab - ba$ s'appelle leur *commutateur* (*annulaire*). Comme en théorie des groupes, on peut dire que le commutateur est la mesure de la non-commutativité (cf. n° 3.2). On vérifie sans difficulté qu'un ensemble A muni d'opérations d'addition, de commutation et de multiplication par des scalaires de k est une algèbre de Lie, dite *associée* à A. L'autre source d'algèbres de Lie — les groupes de Lie — a été mentionnée dans le texte.

Soit maintenant dans l'algèbre associative A un sous-espace L fermé par rapport à la commutation (si bien que, dans l'algèbre de Lie associée, L est une sous-algèbre de Lie). La sous-algèbre associative $\bar{L}$ engendrée dans l'algèbre associative A par l'ensemble L s'appelle algèbre associative *enveloppante* de l'algèbre de Lie L.

Un élément a de l'algèbre linéaire A est appelé *nilpotent* (pour ainsi dire « nul en puissance ») si $a^n = 0$ pour un certain n, généralement dépendant de a, et pour une disposition arbitraire des parenthèses dans a^n. L'algèbre A est dite *nilpotente* s'il existe un n tel que $a_1 \ldots a_n = 0$ pour tous $a_1 \ldots a_n \in A$ et pour une disposition arbitraire des parenthèses dans le premier membre. Le plus petit n possédant cette propriété s'appelle le *degré de nilpotence*. Comme nous l'avons indiqué dans le texte, un exemple d'algèbre associative nilpotente est fourni par l'algèbre des matrices trigonales à diagonale nulle.

26.1.1. Exercice. Toute algèbre nilpotente de type fini est de dimension finie.

26.1.2. Exercice. Une algèbre de Lie L est nilpotente si et seulement si l'on trouve un n tel que $(\ldots((a_1a_2)\,a_3)\ldots)\,a_n = 0$ pour tous $a_1, \ldots, a_n \in L$.

La nilpotence est-elle conservée quand on passe de l'algèbre associative à l'algèbre de Lie et inversement, plus exactement pendant les opérations d'association et d'enveloppement ? Dans le sens direct, la réponse est facile : on comprend que pour une algèbre associative A nilpotente de degré n, l'algèbre de Lie associée sera nilpotente de degré $\leqslant n$ (le signe d'inégalité ne peut pas être supprimé).

Au contraire, l'enveloppement ne conserve pas cette propriété, puisqu'il existe des algèbres associatives non nilpotentes dont les algèbres de Lie associées sont nilpotentes : telle est par exemple l'algèbre A de toutes les matrices trigonales d'un ordre n à diagonales constantes. Un autre exemple : la somme directe B d'algèbres nilpotentes 1-engendrées dont les degrés de nilpotence croissent indéfiniment.

La cause de la non-nilpotence de A saute aux yeux : les éléments isolés de A ne sont même pas tous nilpotents au sens associatif. A condition que les éléments soient associativement nilpotents et que l'algèbre de Lie « enveloppée » soit de type fini, la propriété de nilpotence sera conservée après l'enveloppement :

26.1.3. Théorème. *Soient A une algèbre associative et L un sous-espace de A fermé par rapport à la commutation. Si l'algèbre de Lie L est nilpotente et de type fini et si chacun de ses éléments est nilpotent au sens associatif, l'algèbre associative enveloppante $\bar{L}$ est nilpotente.*

Démonstration. Soient $e_1, \ldots, e_s$ les générateurs de l'algèbre de Lie L. Appelons-les commutateurs générateurs de poids 1, et si l'on connaît déjà des commutateurs générateurs c, d de poids u, v, appelons le commutateur (c, d) commutateur générateur de poids $u + v$ (on voit donc que le poids ne dépend pas seulement de l'élément mais aussi du mode d'écriture). Soit n le degré de nilpotence de l'algèbre de Lie L. Cela signifie que les commutateurs de poids $\geqslant n$ sont nuls, aussi l'ensemble des commutateurs générateurs non nuls est-il fini. Ordonnons cet ensemble par croissance des poids, et si les poids sont les mêmes, par un procédé quelconque : $c_1, c_2, \ldots$ $\ldots, c_r$. Par définition, $c_i^{n_i} = 0$ pour un certain n_i. Montrons que l'algèbre associative $\bar{L}$ est nilpotente de degré au plus égal à $N = n(n_1 + \ldots + n_r)$. Pour le faire, il suffit évidemment de vérifier que tous les $c_{i_1} \ldots c_{i_N} = 0$.

Nous dirons que la *longueur* du produit $c_{i_1} \ldots c_{i_m}$ est le nombre m ; son *poids*, la somme des poids des facteurs ; son *désordre*, tout cas de succession de facteurs $\ldots c_i \ldots c_j \ldots$ où $i > j$; sa *caractéristique*, le couple (m, t), où t est le nombre des désordres. Disposons les caractéristiques dans l'ordre lexicographique, i.e. posons $(m, t) < (m', t')$ chaque fois que $m < m'$ ou que $m = m'$, $t < t'$. Il est évident que toute suite de caractéristiques strictement décroissante est stationnaire.

Si le produit $c_{i_1} \ldots c_{i_N}$ de poids w admet un désordre $c_i c_j$, il suffit de remplacer ce dernier par $c_j c_i + (c_i, c_j)$ pour obtenir une somme de deux produits de même poids mais de caractéristiques infé-

rieures. Donc, au bout d'un nombre fini de remplacements de ce type, on obtiendra une somme de produits

$$c_{j_1}^{m_1} \dots c_{j_l}^{m_l}, \text{ où } j_1 < \dots < j_l \text{ et tous les } m_\alpha \geqslant 1.$$

Il ne reste qu'à remarquer que pour $w \geqslant N$ les produits indiqués sont nuls. En effet, pour $w \geqslant N$ on a un $m_\alpha \geqslant n_{j_\alpha}$, auquel cas $c_{j_\alpha}^{m_\alpha} = 0$. Le théorème est démontré.

Avant de terminer ce n°, citons un résultat sur le type fini pour les anneaux qui rappelle l'exercice 14.3.2 pour les groupes. Bien que la nilpotence n'intervienne pas explicitement dans son énoncé, ce résultat est très utile pour l'étude de la nilpotence, ce qui justifie son apparition ici. D'autre part, nous en aurons besoin ailleurs (voir § 21).

Rappelons qu'un groupe abélien A pour l'addition est appelé *module à gauche* sur l'anneau k si pour tous $\alpha \in k$, $a \in A$ on a un $\alpha a \in A$ et si les quatre premiers axiomes de la liste citée tout au début du paragraphe sont vérifiés. Un *module à droite* se définit d'une façon analogue. Si A est muni d'une structure de module à gauche et à droite sur k et si $(\alpha a)\beta = \alpha(a\beta)$ pour tous $\alpha, \beta \in k$, $a \in A$, on dit que A est un *bimodule* sur k. On appelle *annulateur* du bimodule A sur k l'ensemble de tous les $\alpha \in k$ tels que

$$\alpha a = 0, \quad a\alpha = 0 \text{ pour tout } a \in A.$$

Soient K un anneau associatif (pas nécessairement commutatif), M une partie de K, s un entier naturel. Alors M^s désigne le sous-groupe du groupe additif de K, engendré par tous les produits de s éléments de M.

26.1.4. Théorème. *Soit I un idéal d'un anneau associatif K de type fini. Si le groupe additif K/I est de type fini, l'idéal I est de type fini et tous les groupes additifs K/I^s, $s = 1, 2, \dots$, sont de type fini, eux aussi.*

Démonstration. a) Choisissons dans le groupe additif de l'anneau K un sous-groupe de type fini A tel que

$$K = A + I, \quad K \text{ engendré par } A. \tag{1}$$

Soit I' l'idéal engendré dans K par l'intersection $I \cap (A + A^2)$. La somme $A + I'$ est un sous-anneau. En effet, si $a_1, a_2 \in A$, on a en vertu de (1) $a_1 a_2 = a + i$, $a \in A$, $i \in I$. On a évidemment $i \in I'$, si bien que $a_1 a_2 \in A + I'$.

D'où $K = A + I'$ (voir (1)). Puisque A est de type fini, le groupe additif K/I' l'est aussi, de même que son sous-groupe I/I'.

De la définition de l'idéal I' on voit qu'il est de type fini, car $A + A^2$ est un groupe additif de type fini. Par conséquent, l'idéal I est de type fini.

b) L'anneau K opère sur le groupe additif I/I^2 par multiplications à gauche et à droite, en transformant ce groupe en bimodule sur K. Il est clair que I est contenu dans son annulateur, si bien que I/I^2 peut être considéré comme un bimodule sur K/I ; en outre, il est de type fini en vertu de a). Puisque le groupe additif K/I est de type fini, le groupe additif I/I^2 l'est aussi. Par récurrence sur n on voit que tous les groupes additifs K/I^{2^n} sont de type fini. Enfin, pour tout s il existe un n tel que $2^n > s$, si bien que tous les groupes additifs K/I^s sont de type fini. Le théorème est démontré.

26.2. Les nil-algèbres non nilpotentes. Nous ne considérerons, dans ce n°, que des algèbres associatives. Si tous les éléments d'une algèbre sont nilpotents, elle s'appelle une *nil-algèbre*. Une des questions de fond de la théorie des nil-algèbres est la suivante : une nil-algèbre associative de type fini est-elle nilpotente ? Pour les algèbres de dimension finie, on a obtenu depuis longtemps la réponse positive ; or, si la condition de dimension finie n'est pas imposée à priori, E.S. Golod a montré que la réponse sera négative. Plus exactement, E.S. Golod a construit pour tout corps commutatif k et tout $d \geqslant 2$ une algèbre non nilpotente sur k à d générateurs, telle que toutes ses sous-algèbres à $d - 1$ générateurs sont nilpotentes (*Izv. AN SSSR*, série math., 1964, 28, n° 2, p. 273-276). Sa construction permet de donner les réponses à quelques questions importantes relevant de la théorie des groupes. Le but que nous nous donnons dans ce n° consiste à décrire cette construction.

Soit $F = k\{x_1, \ldots, x_d\}$ un anneau de polynômes sur un corps commutatif k en variables non permutables $x_1, \ldots, x_d$. Il est évident que F se décompose en somme directe $F_0 \oplus F_1 \oplus \ldots$, où $F_0 \simeq k$, F_n est un espace vectoriel engendré sur k par d^n monômes $x_{i_1}x_{i_2} \ldots x_{i_n}$. Les polynômes de F_n sont dits *homogènes* de degré n. Un idéal I de l'anneau F est dit *homogène* s'il est engendré par des polynômes homogènes (de degrés différents en général).

26.2.1. Exercice. Un idéal I est homogène si et seulement si, avec son élément quelconque, il contient toutes ses composantes homogènes, i.e. si

$$a \in I,\ a = a_{n_1} + \ldots + a_{n_s},\ a_{n_i} \in F_{n_i},\ n_1 < \ldots < n_s,$$

implique que tous les $a_{n_i} \in I$.

Soient $f_1, f_2, \ldots$ des polynômes homogènes non nuls de F aux degrés croissants $\geqslant 2$, le nombre r_n des polynômes de chaque degré donné n étant fini. Soient I un idéal engendré par les éléments

$f_1, f_2, \ldots$, et $A = F/I$. Il est évident que $A = A_0 \oplus A_1 \oplus \ldots$, où $A_n = (F_n + I)/I$. En particulier, $A_0 \simeq F_0 \simeq k$, $A_1 \simeq F_1$, car les polynômes f_i sont de degrés $\geqslant 2$. L'élément fondamental de la construction décrite est l'algèbre quotient F/I par un idéal I. En préparant cette construction, nous allons établir un critère de sa dimension infinie.

Considérons une série de puissances formelle

$$\mathfrak{s} = 1 - dt + \sum_{n=2}^{\infty} s_n t^n,$$

où les s_n sont des entiers. On comprend sans peine que la série inverse sera

$$\mathfrak{s}^{-1} = \sum_{n=0}^{\infty} y_n t^n,$$

où

$$y_0 = 1, \quad y_1 = d,$$

$$y_n = dy_{n-1} - \sum_{i=2}^{n} s_i y_{n-i}, \quad n = 2, 3, \ldots$$

26.2.2. Théorème (E.S. Golod). *Soit $F = k\{x_1, \ldots, x_d\}$ un anneau de polynômes sur le corps commutatif k en variables non permutables $x_1, \ldots, x_d$. Soient $f_1, f_2, \ldots$ des polynômes homogènes de F aux degrés croissantes $\geqslant 2$, et I un idéal engendré par eux. Si le nombre r_n des polynômes de degré n parmi $f_1, f_2, \ldots$ est inférieur à s_n et si tous les coefficients de la série $\mathfrak{s}^{-1}$ sont positifs, l'algèbre F/I est de dimension infinie.*

Démonstration. a) Soit a_n la dimension de l'algèbre quotient $A_n = (F_n + I)/I$ considérée comme un espace vectoriel sur k. Pour démontrer ce théorème, il suffit de s'assurer que la série

$$\mathfrak{a} = \sum_{n=0}^{\infty} a_n t^n$$

n'est pas un polynôme. Soit

$$\mathfrak{r} = 1 - dt + \sum_{n=2}^{\infty} r_n t^n;$$

supposons démontré que les séries $\mathfrak{r}^{-1}$ et $\mathfrak{r}\mathfrak{a}$ ont les coefficients positifs (nous le ferons un peu plus tard). Puisque $\mathfrak{r}^{-1}\mathfrak{r} = 1$, on a

$$\mathfrak{r}^{-1}\left(1 + \sum_{n=2}^{\infty} r_n t^n\right) = 1 + \mathfrak{r}^{-1} dt.$$

On voit donc que τ^{-1} n'est pas un polynôme. Par suite, $\alpha = \tau^{-1} \cdot \tau\alpha$ n'est pas un polynôme, elle non plus.

b) La série τ^{-1} a les coefficients positifs. En effet, on a en vertu des propriétés évidentes des opérations sur des séries formelles

$$\tau = \xi - \mathfrak{q} = \xi(1 - \xi^{-1}\mathfrak{q}), \text{ où } \mathfrak{q} = \sum_{n=2}^{\infty} (s_n - r_n)\, t^n,$$

et par conséquent

$$\tau^{-1} = \xi^{-1}(1 - \xi^{-1}\mathfrak{q})^{-1} = \xi^{-1}\left(1 + \sum_{m=1}^{\infty} (\xi^{-1}\mathfrak{q})^m\right).$$

Ceci noté, rappelons que les séries ξ^{-1} et $\mathfrak{q}$ ont les coefficients positifs.

c) Montrons que la série $\tau\alpha$ a les coefficients positifs, elle aussi, i.e. que

$$a_n \geqslant d a_{n-1} - \sum_{i=2}^{n} r_i a_{n-i}, \quad n \geqslant 2. \tag{2}$$

Soient I_n l'ensemble de tous les polynômes homogènes de degré n dans I, A_n^* le supplémentaire du sous-espace I_n dans l'espace F_n, i.e. $F_n = I_n \oplus A_n^*$. La comparaison des dimensions permet de voir que

$$d^n = \dim I_n + a_n.$$

Soient en outre H_m le sous-espace engendré par les polynômes de degré m parmi $f_1, f_2, \ldots$, et XY le sous-espace engendré par les éléments xy, $x \in X$, $y \in Y$. Nous montrerons que

$$I_n \subseteq I_{n-1}F_1 + \sum_{m=2}^{n} A_{n-m}^* H_m, \quad n \geqslant 2. \tag{3}$$

Le calcul des dimensions dans (3) nous donnera précisément (2).

Soit $u \in I_n$. Par construction, u est une somme de produits de la forme vf_jw, où v, w sont des polynômes homogènes. Supposons que $u = vf_jw$. Si w est de degré $\geqslant 1$, il est clair que $u \in I_{n-1}F_1$. Par contre, si f est de degré 0, on peut admettre que $u = vf_j$. Supposons que f_j soit de degré m, donc appartienne au sous-espace H_m. Alors $v \in F_{n-m}$,

$$v = v' + v'', \quad v' \in I_{n-m}, \quad v'' \in A_{n-m}^*.$$

D'où $u \in I_{n-1}F_1 + A_{n-m}^* H_m$. Le théorème est démontré.

26.2.3. Exemple. Si dans les conditions du théorème 26.2.2

$$r_n \leqslant \varepsilon^2 (d - 2\varepsilon)^{n-2}, \quad \varepsilon > 0, \tag{4}$$

l'algèbre A est de dimension infinie. En effet, il suffit de s'assurer que la série $\mathfrak{z}^{-1}$ a les coefficients positifs, où

$$\mathfrak{z} = 1 - dt + \sum_{n=2}^{\infty} \varepsilon^2 (d - 2\varepsilon)^{n-2} t^n.$$

Nous utiliserons les formules suivantes pour les séries formelles:

$$\frac{1}{1-a} = \sum_{n=0}^{\infty} a^n, \quad \frac{1}{(1-a)^2} = \sum_{n=0}^{\infty} (n+1)\, a^n.$$

Il vient

$$\mathfrak{z} = 1 - dt + \varepsilon^2 t^2 \sum_{n=0}^{\infty} (d - 2\varepsilon)^n t^n =$$

$$= 1 - dt + \frac{\varepsilon^2 t^2}{1 - (d - 2\varepsilon)\, t} = \frac{(1 - (d - \varepsilon)\, t)^2}{1 - (d - 2\varepsilon) t},$$

d'où

$$\mathfrak{z}^{-1} = \frac{1 - (d - 2\varepsilon)\, t}{(1 - (d - \varepsilon)\, t)^2} =$$

$$= (1 - (d - 2\varepsilon)\, t) \sum_{n=0}^{\infty} (n+1)\, (d - \varepsilon)^n t^n =$$

$$= 1 + \sum_{n=1}^{\infty} (d - \varepsilon)^{n-1} (d + (n-1)\, \varepsilon)\, t^n.$$

Puisque $d - 2\varepsilon \geqslant 0$, on a $d - \varepsilon \geqslant \varepsilon > 0$, ce qui achève la démonstration.

Maintenant nous pouvons décrire la construction de E.S. Golod. Son idée ressort clairement dans le cas particulier suivant.

26.2.4. Exemple. Soient k un corps commutatif au plus dénombrable, $F = k\{x, y\}$ une algèbre de polynômes sur k en variables non permutables x, y, F' sa sous-algèbre des polynômes sans terme constant. Montrons qu'il existe dans F un idéal I inclus dans F' tel que l'algèbre $A' = F'/I$ est non nilpotente, bien que tous ses éléments (donc aussi toutes ses sous-algèbres 1-engendrées) soient nilpotents.

Numérotons les éléments de F' : $u_1, u_2, \ldots$ Soit $N_1 = 9$. Elevons u_1 à la puissance N_1 et décomposons $u_1^{N_1}$ en somme de termes homogènes $f_1, f_2, \ldots, f_{m_1}$ aux degrés strictement croissants. Soit N_2 strictement supérieur à tous les degrés des termes. Elevons u_2 à la puissance N_2 et décomposons $u_2^{N_2}$ en somme de termes homogènes $f_{m_1+1}, f_{m_1+2}, \ldots$ aux degrés strictement croissants. Poursuivant

ce processus, nous obtiendrons des polynômes $f_1, f_2, \ldots$ aux degrés strictement croissants $\geqslant 9$. Soit I l'idéal engendré par ces polynômes. Il est clair que $A' = F'/I$ est une nil-algèbre à générateurs $\bar{x} = x + I$, $\bar{y} = y + I$. Il reste à vérifier que A' n'est pas nilpotente; à cet effet, il suffit de s'assurer que $A = F/I$ est de dimension infinie (auquel cas $A' = A_1 \oplus A_2 \oplus \ldots$ est aussi de dimension infinie, donc non nilpotente; voir l'exercice 26.1.1). Avec les notations du théorème de Golod on a $d = 2$, $r_n \leqslant 1$, de telle façon que $r_2 = r_3 = \ldots = r_s = 0$. Un calcul direct montre que pour $\varepsilon = 1/4$ la condition de l'exemple 26.2.3 est vérifiée, d'où la proposition.

Exposons maintenant le résultat de E.S. Golod dans le cas général.

26.2.5. Exemple. Pour tout $d \geqslant 2$ et tout corps commutatif k, il existe une algèbre non nilpotente sur k à d générateurs dont toute sous-algèbre à $d - 1$ générateurs est nilpotente. En effet, soient $F = k\{x_1, \ldots, x_d\}$ une algèbre de polynômes sur k en variables non permutables $x_1, \ldots, x_d$, F' sa sous-algèbre des polynômes sans terme constant. Construisons dans F un idéal I inclu dans F' tel que F'/I soit l'algèbre cherchée.

Soit ε un nombre donné, $0 < \varepsilon < 1/2$. Conformément à l'exemple 26.2.3, on peut prendre comme I l'idéal engendré par des polynômes homogènes $f_1, \ldots, f_{s_1}, f_{s_1+1}, \ldots, f_{s_2}, \ldots$ de degré $\geqslant 2$ vérifiant la condition (4) et la condition auxiliaire suivante: pour $d - 1$ éléments quelconques de degré $\leqslant n$ dans F', il existe un entier naturel N tel que le produit de N facteurs quelconques parmi ces éléments appartient à l'idéal I_n engendré par les éléments $f_1, \ldots, f_{s_n}$. Supposons que le segment $f_1, \ldots, f_s$, $s = s_{n-1}$, soit déjà construit et montrons qu'on peut le compléter en le segment $f_1, \ldots, f_t$, $t = s_n$.

Considérons $d - 1$ polynômes de degré $\leqslant n$ sans terme constant à coefficients indéterminés (littéraux) $c_{i\alpha}$:

$$g_i = \sum_\alpha c_{i\alpha} M_\alpha (x_1, \ldots, x_d), \quad 1 \leqslant i \leqslant d - 1,$$

où M_α sont des monômes. Soit N un entier naturel. Il existe $(d-1)^N$ produits distincts de N éléments g_i. En les écrivant sous la forme de polynômes en $\{c_{i\alpha}\}$, on obtient comme coefficients des combinaisons linéaires $f_{s+1}, \ldots, f_t$ de monômes en $\{x_j\}$ de degrés $N, N+1, \ldots, nN$. Montrons que pour un N suffisamment grand, $f_{s+1}, \ldots, f_t$ sont les polynômes cherchés. Il est clair que seule la propriété (4) est à vérifier. Elle a lieu à condition de prendre N plus grand que les degrés de $f_1, \ldots, f_s$ et tel que le nombre des polynômes $f_{s+1}, \ldots, f_t$ soit inférieur à $\varepsilon^2 (d - 2\varepsilon)^{N-2}$. Montrons qu'un tel N existe. A cet effet, majorons le nombre des polynômes $f_{s+1}, \ldots, f_t$ en fonction de N.

Soit $g = g_{i_1} \ldots g_{i_N}$, où g_i intervient m_i fois dans le produit. Puisque les $c_{i\alpha}$ commutent (ce sont les symboles littéraux désignant les éléments du corps commutatif k), le nombre des termes de g, qui est un polynôme en $\{c_{i\alpha}\}$, est égal à

$$\prod_{i=1}^{d-1} \binom{m_i+q-1}{q-1}, \quad q=d+d^2+\ldots+d^n.$$

Il y a donc autant de polynômes ajoutés par le produit g au segment $f_{s+1}, \ldots, f_t$. Puisque $\binom{u}{v} \leqslant u^v$ et qu'il existe $(d-1)^N$ produits g distincts, le nombre total des polynômes $f_{s+1}, \ldots, f_t$ n'est pas supérieur à

$$(d-1)^N (N+q-1)^{(q-1)(d-1)}.$$

Puisque $d-1 < d-2\varepsilon$, ce nombre est inférieur à $\varepsilon^2 (d-2\varepsilon)^{N-2}$ pour un N suffisamment élevé, ce qui achève la démonstration.

§ 27. Théorèmes locaux de la logique

Nous établirons ici le théorème local de Maltsev pour les classes quasi universelles. Supposant que le lecteur connaît les définitions fondamentales du cours général de logique formelle, nous nous bornerons à donner un exposé un peu sommaire mais parfaitement « clos ».

27.1. Systèmes algébriques. Soit A un ensemble. On appelle *prédicat n-aire* (resp. *opération n-aire*) sur A une fonction de n variables définie sur A à valeurs dans l'ensemble $\{vrai, faux\}$ (resp. dans A). L'ensemble A muni de prédicats $P_\alpha^{n_\alpha}$ et d'opérations $f_\beta^{m_\beta}$ (n_α, m_β étant leurs arités) s'appelle *système algébrique*, et la liste des symboles $P_\alpha^{n_\alpha}$, $f_\beta^{m_\beta}$ sa *signature*. Deux systèmes algébriques de même signature sont dits *isomorphes* s'il existe entre eux une correspondance biunivoque conservant prédicats et opérations. Les exemples de systèmes algébriques sont donnés par les groupes, les anneaux, les corps commutatifs, les espaces vectoriels, les ensembles ordonnés, etc.

Une partie d'un système algébrique, fermée pour toutes les opérations de signature s'appelle *sous-système* si elle est considérée avec les prédicats et les opérations induits sur elle par restriction des prédicats et des opérations de signature du système lui-même.

Il a été dit dans le texte qu'un ensemble de parties A_i, $i \in I$, d'un ensemble A s'appelle *recouvrement local* de A si tout élément de A appartient à un A_i et si deux ensembles quelconques A_i, A_j sont contenus dans un troisième ensemble A_k. Les recouvrements locaux sont étroitement liés à la notion de filtre.

Soit I un ensemble. Un système F de ses parties non vides est dit *centré* s'il est fermé pour les intersections finies: $X \in F, Y \in F \Rightarrow \Rightarrow X \cap Y \in F$. Un système centré F s'appelle *filtre* sur I si, avec chaque son ensemble, il contient tous les surensembles de ce dernier: $X \in F, Y \supseteq X \Rightarrow Y \in F$. Un filtre est appelé *ultrafiltre* s'il n'est contenu dans aucun filtre plus grand que lui. On vérifie sans peine que cette dernière condition équivaut à ce qui suit: étant donnée une partie de I, F contient soit cette partie, soit son complémentaire. On peut évidemment compléter tout système centré en un filtre (en y ajoutant les surensembles de tous ses ensembles) et tout filtre en un ultrafiltre (lemme de Zorn). Remarquons en passant qu'on ne connaît jusqu'à présent aucun ultrafiltre construit autrement que par le lemme de Zorn, sauf un filtre dénué d'intérêt qui réunit tous les surensembles d'un point.

Soit A_i, $i \in I$, un recouvrement local de l'ensemble A. Pour tout $\alpha \in I$, posons

$$I_\alpha = \{i \mid i \in I,\ A_i \supseteq A_\alpha\}.$$

Il est facile de voir que l'intersection $I_\alpha \cap I_\beta$ contient un I_γ. Donc, le système de tous les I_α peut être centré et, par conséquent, il existe un ultrafiltre F qui contient ce système. Si chaque A_i est muni d'un prédicat P_i, désignons par $P = \lim P_i$ le prédicat défini sur A par la formule suivante:

$$P\ (x,\ y,\ \ldots) = \mathrm{V} \text{ sur } A \Leftrightarrow$$
$$\Leftrightarrow \{i \mid x,\ y,\ \ldots \in A_i,\ P_i\ (x,\ y,\ \ldots) = \mathrm{V} \text{ sur } A_i\} \in F.$$

En général, la restriction de P à A_i ne se confond pas nécessairement avec P_i. Or, en prenant un prédicat défini sur A, en faisant sa restriction à chaque A_i et en passant à la limite suivant le filtre F au sens défini ci-dessus, on retrouve bien sûr le prédicat initial.

27.2. Langage du calcul des prédicats. L'alphabet du langage CP comprend les variables d'objet et de prédicat, les parenthèses et sept symboles logiques dont les quatre premiers s'appellent *connecteurs* et les deux derniers *quantificateurs*:

$\wedge$	et
$\vee$	ou
$\neg$	non
$\rightarrow$	implique
$=$	égal
$\forall$	quel que soit
$\exists$	il existe

Les formules de CP qui sont exemptes de quantificateurs appliqués aux prédicats s'appellent *formules de calcul des prédicats restreint*

(CPR). Malgré la pauvreté du vocabulaire, le langage CP est très efficace. Par exemple, la classe des groupes abéliens sans torsion se laisse définir par les axiomes suivants de CP (voir de CPR) dans la signature usuelle $\cdot$, $^{-1}$, e de la théorie des groupes:

1° l'associativité: $(\forall x)\ (\forall y)\ (\forall z)\ ((xy)\ z = x\ (yz))$,

2° l'existence de l'unité: $(\forall x)\ (xe = x \wedge ex = x)$,

3° l'existence des éléments inverses: $(\forall x)\ (x^{-1}x = e \wedge xx^{-1} = e)$,

4° la commutativité: $(\forall x)\ (\forall y)\ (xy = yx)$,

5° l'absence de la torsion: $(\forall x)\ (x = e \wedge \neg\ (\underbrace{x\ \ldots\ x}_{n} = e))$,

$n = 1, 2, \ldots$

Citons encore quelques exemples. Un prédicat binaire est appelé *ordre partiel* s'il vérifie les propriétés suivantes:

6° la réflexivité: $(\forall x)\ (x \leqslant x)$,

7° l'antisymétrie: $(\forall x)\ (\forall y)\ (x \leqslant y \wedge y \leqslant x \rightarrow x = y)$,

8° la transitivité: $(\forall x)\ (\forall y)\ (\forall z)\ (x \leqslant y \wedge y \leqslant z \rightarrow x \leqslant z)$, et *ordre total* s'il vérifie en outre

9° la relation d'ordre total: $(\forall x)\ (\forall y)\ (x \leqslant y \vee y \leqslant x)$. Un prédicat $\leqslant$ défini sur un groupe est dit *stable pour la multiplication* si

10° $(\forall x)\ (\forall y)\ (\forall z)\ (x \leqslant y \rightarrow xz \leqslant yz \wedge zx \leqslant zy)$. On appelle *groupe ordonnable* un groupe qui admet un ordre total stable pour la multiplication. Un groupe est dit *préordonnable* si son ordre partiel quelconque stable pour la multiplication se laisse prolonger en un ordre total stable pour la multiplication. On comprend sans difficulté que les classes des groupes ordonnables et préordonnables sont définies dans la classe de tous les groupes par les axiomes suivants de CP (mais non de CPR comme précédemment):

11° l'ordonnabilité: $(\exists P)\ (\forall x)\ (\forall y)\ (\forall z)\ (P\ (x, x) \wedge (P\ (x, y) \wedge \wedge\ P\ (y, x) \rightarrow x = y) \wedge (P\ (x, y) \wedge P\ (y, z) \rightarrow P\ (x, z)) \wedge \wedge\ (P\ (x, y) \vee P\ (y, x)) \wedge (P\ (x, y) \rightarrow P\ (xz, yz) \wedge P\ (zx, zy)))$,

12° la préordonnabilité: $(\forall P)\ ((P = \text{o.p.s.}) \rightarrow (\exists Q)\ ((Q = = \text{o.t.s.}) \wedge (\forall u)\ (\forall v)\ (P\ (u, v) \rightarrow Q\ (u, v))))$. Dans cette dernière formule, faute de place, nous n'avons pas écrit explicitement les axiomes d'ordre partiel stable et ceux d'ordre total stable, qui s'obtiennent sans peine en combinant les axiomes 6°-10°.

Rappelons qu'on peut transformer canoniquement toute formule de CP en une *formule prénexe* équivalente, i.e. une formule où les quantificateurs précèdent tous les autres symboles logiques. La formule prénexe est appelée *universelle* si elle ne contient aucun quantificateur $\exists$, et *objet-universelle* si aucun de ses quantificateurs $\exists$ ne s'applique à une variable d'objet. La formule de CP est dite *quasi universelle* si elle se déduit à partir de formules objet-universelles sans variables d'objet libres par la seule utilisation de connecteurs, suivie de la préfixation des quantificateurs $\forall$ aux variables d'objet libres (cette définition diffère quelque peu de la définition originale

de A.I. Maltsev (1959) ; elle a été proposée par J.P. Cleave (*J. London Math. Soc.* (1), 1969, 44, n° 1, p. 121-130 ; Addendum. — *J. London Math. Soc.* (2), 1969, 1, n° 2, p. 384) qui a donné à ces formules l'appellation *boolean-universal*). Les exemples de formules universelles sont donnés par les formules 1° à 10°. La formule 11° est objet-universelle, la formule 12° est équivalente à une formule quasi universelle qu'on obtient en transportant les préfixes de quantification du domaine d'action du préfixe $(\exists Q)$ immédiatement derrière $(\exists Q)$.

27.2.1. Exercice. Les groupes simples se définissent dans la classe de tous les groupes par un axiome quasi universel.

27.3. Théorèmes locaux. Considérons d'abord les formules objet-universelles.

27.3.1. Théorème. *Soit Φ une formule objet-universelle. Si Φ est vraie sur un système algébrique A, elle reste vraie sur tout sous-système A_i de A. Si Φ est vraie sur les sous-systèmes A_i recouvrant localement A, elle reste vraie sur A.*

Démonstration. Pour éviter les fastidieuses notations « universelles », bornons-nous au cas où la signature se réduit à un symbole d'opération binaire $\cdot$ et à un symbole de prédicat binaire S.

a) Soit A un système algébrique de signature indiquée, vérifiant un axiome objet-universel Φ, et soit A' un sous-système de A, i.e. sa partie munie du prédicat induit et de l'opération induite, qui est fermée pour cette dernière. Montrons que Φ reste vrai sur A'. Supposons d'abord que Φ soit exempt de quantificateurs. La proposition résulte alors immédiatement de la définition du vrai (rappelons que, par définition, une formule de CP est vraie sur un système algébrique si et seulement si elle reste vraie, quelles que soient les valeurs des variables d'objet et de prédicat non quantifiées). Supposons maintenant que Φ contienne des quantificateurs et raisonnons par récurrence sur leur nombre. Trois cas sont à distinguer suivant que la dernière position est occupée par tel ou tel quantificateur : 1° $\Phi = (\forall t)\ \Psi$, 2° $\Phi = (\forall T)\ \Psi$, 3° $\Phi = (\exists T)\ \Psi$, où t est une variable d'objet et T une variable de prédicat. Prolongeant la définition des prédicats de A' à A tout entier ou, au contraire, faisant la restriction de A à A' et appliquant l'hypothèse de récurrence dans les trois cas, nous constatons que Φ reste vrai sur A'.

b) Supposons que les sous-systèmes A_i, $i \in I$, recouvrent localement le système algébrique A et vérifient la formule Φ. On demande de montrer que Φ reste vraie sur A. Supposons que Φ contienne des variables d'objet libres x, y, . . . et des variables de prédicat libres P, Q, . . . :

$$\Phi = \Phi\ (x,\ y,\ \ldots,\ P,\ Q,\ \ldots).$$

Soit F un ultrafiltre quelconque sur I construit à partir du recouvrement local A_i, $i \in I$, de la façon indiquée en fin du n° 27.1. Choisissons sur chaque A_i des prédicats $P_i, Q_i, \ldots$ et posons $P_0 = \lim P_i$, $Q_0 = \lim Q_i, \ldots$ Pour démontrer le théorème, il suffit de s'assurer que pour toutes les valeurs de $x, y, \ldots$ de A on a

$$\{i \mid x, y, \ldots \in A_i, \Phi(x, y, \ldots, P_i, Q_i, \ldots) = \\ = \mathrm{V} \text{ sur } A_i\} \in F \Rightarrow \Phi(x, y, \ldots, P_0, Q_0, \ldots) = \mathrm{V} \text{ sur } A. \quad (1)$$

Afin de raisonner par récurrence sur le nombre des quantificateurs, supposons d'abord que Φ soit sans quantificateurs et montrons qu'on a alors (1), ainsi que l'implication réciproque. Soit (1′) la réunion de ces implications. Si la formule Φ est sans connecteurs, trois cas sont à distinguer: 1° $\Phi = (u(x, y, \ldots) = v(x, y, \ldots))$, 2° $\Phi = S(u, v)$, 3° $\Phi = P(u, v, \ldots)$, où u, v sont des produits avec une disposition donnée des parenthèses. Dans les deux premiers cas, (1′) est immédiate et dans le troisième cas elle découle de la définition de lim. Supposons maintenant que Φ soit comme précédemment sans quantificateurs mais qu'elle contienne des connecteurs. Puisque $\Psi \to \Omega$ équivaut à $\neg\Psi \vee \Omega$, supposons que Φ ne contienne que des connecteurs $\wedge$, $\vee$, $\neg$ et démontrons (1′) par récurrence sur leur nombre. Trois cas sont à distinguer selon qu'on a tel ou tel connecteur en dernière position: 4° $\Phi = \Psi \wedge \Omega$, 5° $\Phi = \Psi \vee \Omega$, 6° $\Phi = \neg\Psi$. Dans chaque cas, (1′) découle facilement de l'hypothèse de récurrence et de la définition du filtre F.

Supposons enfin que Φ contienne des quantificateurs et démontrons la proposition (1) par récurrence sur leur nombre. Selon qu'on a tel ou tel quantificateur en dernière position, trois cas sont à distinguer: 7° $\Phi = (\forall t)\Psi$, 8° $\Phi = (\forall T)\Psi$, 9° $\Phi = (\exists T)\Psi$, où t est une variable d'objet et T une variable de prédicat. Examinons le cas 7°. Supposons que t prenne une valeur dans A. Il s'agit de montrer que $\Psi(t, x, y, \ldots, P_0, Q_0, \ldots) = \mathrm{V}$ sur A. Par hypothèse de récurrence, il suffit alors de s'assurer que l'ensemble

$$\{i \mid t, x, y, \ldots \in A_i, \Psi(t, x, y, \ldots, P_i, Q_i, \ldots) = \mathrm{V} \text{ sur } A_i\}$$

appartient à F. Or, cet ensemble contient l'intersection de l'ensemble $\{\ldots\}$ de (1) avec l'ensemble $\{i \mid t \in A_i\}$, d'où la proposition. Passons au cas 8°. Soient T_0 un prédicat quelconque sur A, et T_i sa restriction à A_i. Comme nous l'avons dit en fin du n° 27.1, $T_0 = \lim T_i$. On veut montrer que

$$\Psi(x, y, \ldots, T_0, P_0, Q_0, \ldots) = \mathrm{V} \text{ sur } A.$$

Par hypothèse de récurrence, il suffit de s'assurer que l'ensemble

$$\{i \mid x, y, \ldots \in A_i, \Psi(x, y, \ldots, T_i, P_i, Q_i, \ldots) = \mathrm{V} \text{ sur } A_i\}$$

appartient à F. Or, cet ensemble contient $\{\ldots\}$ de (1), d'où la pro-

position. Plaçons-nous enfin dans le dernier cas 9°. Supposons que la prémisse dans (1) soit vraie. Il existe alors sur chaque système A_i un prédicat T_i tel que l'ensemble

$$\{i \mid x, y, \ldots \in A_i,\ \Psi(x, y, \ldots, T_i, P_i, Q_i, \ldots) = \mathrm{V} \text{ sur } A_i\}$$

appartienne à F. Soit $T_0 = \lim T_i$. Par hypothèse de récurrence, $\Psi(x, y, \ldots, T_0, P_0, Q_0, \ldots) = \mathrm{V}$ sur A. Or, cela signifie que la conclusion intervenant dans (1) est vraie. Le théorème est démontré.

Pour illustrer ce théorème, remarquons que le théorème local est vrai dans la classe des groupes ordonnés : il suffit de se rappeler que cette classe se définit par l'axiome objet-universel 11° du n° 27.2.

27.3.2. Exercice. Si chaque sous-groupe de type fini dans un groupe G contient un sous-groupe normal abélien d'indice fini $\leqslant n$, le groupe G lui-même contient un sous-groupe normal abélien d'indice $\leqslant n$.

Considérons maintenant des formules quasi universelles quelconques.

27.3.3. Théorème (A.I. Maltsev). *Si la formule quasi universelle Φ est vraie sur les sous-systèmes A_i qui recouvrent localement un système algébrique A, elle est aussi vraie sur A.*

Démonstration. Par définition d'une formule quasi universelle, on a

$$\Phi = (\forall P_1) \ldots (\forall P_n)\, \Phi',$$

où Φ' est composée au moyen des connecteurs $\wedge$, $\vee$, $\neg$, $\rightarrow$ à partir de formules objet-universelles sans variables d'objet libres mais avec des variables de prédicat libres de la liste $P_1, \ldots, P_n$. Supposons Φ vraie sur chaque A_i et montrons que Φ est vraie sur A. Donnons aux variables de prédicat $P_1, \ldots, P_n$ des valeurs quelconques sur A. Il s'agit de montrer que Φ' est vraie sur A pour ces valeurs de $P_1, \ldots, P_n$, sachant que Φ' est vraie sur chaque A_i pour les valeurs induites de $P_1, \ldots, P_n$. En d'autres termes, on veut démontrer le théorème pour Φ' en considérant $P_1, \ldots, P_n$ comme des prédicats de signature. On apprend dans le premier cours de la logique que Φ' se laisse mettre sous une forme équivalente $\Phi' = \bigwedge \Phi_\alpha$, avec $\Phi_\alpha = \bigvee \Phi_{\alpha\beta}$, où $\Phi_{\alpha\beta}$ est une formule objet-universelle close pour les variables d'objet, ou la négation d'une telle formule. De toute évidence, si le théorème a lieu pour tout Φ_α, il a lieu pour Φ'. Nous pouvons donc nous borner à considérer les trois cas suivants :

1° $\Phi = \Psi_1 \vee \ldots \vee \Psi_r$,
2° $\Phi = \neg \Omega_1 \vee \ldots \vee \neg \Omega_s$,
3° $\Phi = \Psi_1 \vee \ldots \vee \Psi_r \vee \neg \Omega_1 \vee \ldots \vee \neg \Omega_s$,

où Ψ_α, Ω_β sont des formules objet-universelles closes pour les variables d'objet, r, $s \geqslant 1$.

Commençons par le cas 3°. Supposons que Φ soit vraie sur tout A_i mais fausse sur A. Alors toutes les Ψ_α sont fausses sur A et toutes les Ω_β vraies sur A. En vertu de la deuxième assertion du théorème 27.3.1, chaque Ψ_α est fausse sur un $A_{i(\alpha)}$. Supposons que A_i contienne tous les $A_{i(\alpha)}$. En vertu de la première assertion du théorème 27.3.1, chaque Ψ_α est fausse sur A_i, chaque Ω_β est vraie sur A_i. Il s'ensuit que Φ est fausse sur A_i, ce qui contredit l'hypothèse. Les cas 1° et 2° se traitent de même, avec des simplifications évidentes. Le théorème est démontré.

Pour illustrer ce théorème, remarquons que le théorème local est vrai dans la classe des groupes préordonnables et dans celle des groupes simples, voir la formule 12° dans le n° 27.2 et l'exercice 27.2.1.

§ 28. Sur les entiers algébriques

Le lecteur est supposé avoir appris les notions fondamentales et la terminologie de la théorie des corps commutatifs dans le cours d'algèbre générale.

Soit $\overline{\mathbb{Q}}$ la clôture algébrique du corps $\mathbb{Q}$ des nombres rationnels. On dit que les éléments de $\overline{\mathbb{Q}}$ sont des *nombres algébriques*. Un élément de $\overline{\mathbb{Q}}$ s'appelle *entier algébrique* s'il est racine d'un polynôme à coefficients entiers dont le coefficient dominant est 1.

Soit k un corps quelconque de nombres algébriques de degré fini (ou, en tant qu'espace vectoriel, de dimension finie) sur $\mathbb{Q}$, et soit k_0 l'ensemble de tous les entiers algébriques dans k.

28.1.1. Exercice. Pour tout $\alpha \in k$ il existe un $m \in \mathbb{Z}$ tel que $m\alpha \in k_0$.

28.1.2. Exercice. $\mathbb{Q}_0 = \mathbb{Z}$.

28.1.3. Lemme. *k_0 est un sous-anneau dans k.*

Démonstration. Soient $\alpha, \beta \in k_0$, et soit γ l'un quelconque des éléments $\alpha \pm \beta$, $\alpha\beta$. Il s'agit de montrer que $\gamma \in k_0$.

Soient

$$\alpha^l = \sum_{i=0}^{l-1} a_i\alpha^i, \quad a_i \in \mathbb{Z}, \quad \beta^m = \sum_{j=0}^{m-1} b_j\beta^j, \quad b_j \in \mathbb{Z}.$$

On comprend aisément que l'ensemble $\mathfrak{o}$ de tous les éléments de la forme

$$\sum_{i=0}^{l-1} \sum_{j=0}^{m-1} c_{ij}\alpha^i\beta^j, \quad c_{ij} \in \mathbb{Z},$$

est un sous-anneau dans k. Soit $\gamma_1, \ldots, \gamma_t$ une base du groupe additif de $\mathfrak{o}$ et soit $\gamma_r\gamma = \sum_s d_{rs}\gamma_s$, $d_{rs} \in \mathbb{Z}$. Le polynôme caractéristique de

la matrice (d_{rs}) s'annule en γ, c'est pourquoi γ est un entier algébrique. Le lemme est démontré.

Il est évident que pour tout $\alpha \in k$ la translation $x \to x\alpha$, $x \in k$, est une transformation linéaire de l'espace k sur le corps $\mathbb{Q}$. Soient χ_α le polynôme caractéristique de cette transformation et tr α sa trace. D'une façon plus générale, si K est un sous-corps dans $\mathbb{C}$, et L son extension de degré fini, alors pour tout $\alpha \in L$ la transformation $x \to x\alpha$, $x \in L$, est linéaire sur K et sa trace se note $\mathrm{tr}_{L/K}(\alpha)$ (elle appartient bien sûr au corps K).

28.1.4. Lemme. *Si $\alpha \in k_0$, alors χ_α est un polynôme sur $\mathbb{Z}$.*

Démonstration. Soit n le degré de k sur $\mathbb{Q}$. Choisissons une base de k sur $\mathbb{Q}$ et associons à chaque $\gamma \in k$ une matrice $\tilde{\gamma}$ de translation $x \mapsto x\gamma$ par rapport à cette base. Nous obtenons de toute évidence un homomorphisme injectif $k \to \mathbf{M}_n(\mathbb{Q})$. Puisque α est racine d'une équation sur $\mathbb{Z}$ à coefficient dominant 1 il en est de même pour les racines caractéristiques de la matrice $\tilde{\alpha}$. En vertu du lemme 28.1.3, les coefficients du polynôme χ_α sont des entiers algébriques. Conformément aux résultats de l'exercice 28.1.2, ils sont dans $\mathbb{Z}$. Le lemme est démontré.

28.1.5. Lemme. *Soit $\omega_1, \ldots, \omega_n$ une base de k sur $\mathbb{Q}$. La matrice $(\mathrm{tr}\,(\omega_i\omega_j))$ est non dégénérée. Il existe une base $\{\omega_j^*\}$ de k sur $\mathbb{Q}$ duale de $\{\omega_i\}$, i.e. telle que*

$$\mathrm{tr}\,(\omega_i\omega_j^*) = \delta_{ij}.$$

Démonstration. a) Supposons au contraire qu'il existe entre les colonnes de la matrice $(\mathrm{tr}\,(\omega_i\omega_j))$ une relation non triviale à coefficients $\alpha_j \in \mathbb{Q}$. On a alors

$$\omega = \sum \alpha_j\omega_j \neq 0, \quad \mathrm{tr}\,(\omega_i\omega) = 0 \text{ pour tout } 1 \leqslant i \leqslant n.$$

Puisque $\{\omega_i\omega\}$ est aussi une base de k sur $\mathbb{Q}$, on a $1 = \sum \beta_i\omega_i\omega$ pour certains $\beta_i \in \mathbb{Q}$. Le calcul de la trace des deux membres nous donne $n = 0$, ce qui est faux.

b) Cherchons ω_j^* sous la forme

$$\omega_j^* = \sum_l \xi_{jl}\omega_l, \quad \xi_{jl} \in \mathbb{Q}.$$

La condition $\mathrm{tr}\,(\omega_i\omega_j^*) = \delta_{ij}$ se transforme en un système d'équations linéaires pour $\xi_{j1}, \ldots, \xi_{jn}$. En vertu de a) ce système est résoluble. Le lemme est démontré.

28.1.6. Théorème. *Le groupe additif de l'anneau k_0 est de type fini.*

Démonstration. Soit $\omega_1, \ldots, \omega_n$ une base de k sur $\mathbb{Q}$. En vertu de l'exercice 28.1.1, on peut admettre que tous les $\omega_i \in k_0$.

Soit $\{\omega_j^*\}$ la base duale. D'après les résultats de l'exercice 28.1.1, il existe un $m \in \mathbb{Z}$ tel que tous les $m\omega_j^* \in k_0$. Soit γ un élément quelconque de k_0,

$$\gamma = \sum \gamma_i \omega_i, \quad \gamma_i \in \mathbb{Q}.$$

Multipliant cette égalité par $m\omega_j^*$ et prenant la trace des deux membres, nous obtenons $m\gamma_j = \mathrm{tr}(m\gamma\omega_j^*)$. Puisque $m\gamma\omega_j^* \in k_0$, on a $m\gamma_j \in \mathbb{Z}$ (lemme 28.1.4). Nous voyons que le groupe additif de l'anneau k_0 est contenu dans un groupe dont l'ensemble générateur est $\left\{\frac{1}{m}\,\omega_i\right\}$, si bien qu'il est lui-même de type fini (voir l'exercice 8.1.7) Le théorème est démontré.

28.1.7. L e m m e. *Soit K un sous-corps dans $\mathbb{C}$. Pour toute extension L/K de degré d, il existe exactement d isomorphismes de L sur $\mathbb{C}$ identiques sur K. Si $\sigma_1, \ldots, \sigma_d$ sont ces isomorphismes, on a*

$$\mathrm{tr}_{L/K}(\alpha) = \alpha^{\sigma_1} + \ldots + \alpha^{\sigma_d} \text{ pour tout } \alpha \in L. \tag{1}$$

Si $\{\omega_i\}$ est une base de L/K, on a

$$\det(\mathrm{tr}_{L/K}(\omega_i\omega_j)) = \det(\omega^{\sigma_j})^2. \tag{2}$$

D é m o n s t r a t i o n. a) Démontrons d'abord la première assertion. Soient $\alpha \in L$, f le polynôme minimal de l'élément α sur le corps K, $\alpha_1, \ldots, \alpha_m$ les racines de f dans $\mathbb{C}$. Il existe évidemment une correspondance biunivoque entre les isomorphismes $K(\alpha)/K \to \mathbb{C}$ et les applications $\alpha \to \alpha_i$. En vertu du théorème de l'élément primitif (voir [38]), on a $L = K(\alpha)$ pour un α convenablement choisi, d'où l'assertion. Il n'est pas d'ailleurs indispensable de faire appel au théorème de l'élément primitif : il suffit de mettre L sous la forme $K(\gamma_1) \ldots (\gamma_s)$ et de remarquer que tout isomorphisme $K(\gamma_1) \ldots (\gamma_i)/K \to \mathbb{C}$ admet, en vertu de ce qui précède, exactement $|K(\gamma_1) \ldots (\gamma_{i+1}) : K(\gamma_1) \ldots (\gamma_i)|$ prolongements sur $K(\gamma_1) \ldots (\gamma_{i+1})$.

b) Démontrons maintenant (1). Si $L = K(\alpha)$, le polynôme minimal de α sur K est de degré $|L : K|$ et se confond donc avec le polynôme caractéristique de la transformation $x \to x\alpha$ de l'espace vectoriel L sur le corps K.

En vertu de ce qui précède, $\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_d}$ sont exactement ses racines, d'où (1). Le cas général se laisse réduire à celui que l'on vient de considérer, à l'aide de la formule

$$\mathrm{tr}_{L/K}(\alpha) = |L : K(\alpha)| \cdot \mathrm{tr}_{K(\alpha)/K}(\alpha).$$

Démontrons-la. Soient $\{\omega_i\}$ une base de $L/K(\alpha)$, et $\{\delta_j\}$ une base de $K(\alpha)/K$. Alors $\{\omega_i\delta_j\}$ est une base de L/K par rapport à laquelle la matrice de la transformation $x \to x\alpha$ est de forme diagonale par blocs, ces blocs étant occupés par des répétitions de la matrice de cette transformation par rapport à la base $\{\delta_j\}$.

c) Démontrons enfin (2). En vertu de (1) on a

$$\mathrm{tr}_{L/K}(\omega_i\omega_j) = \sum_{\sigma} \omega_i^{\sigma}\omega_j^{\sigma}$$

aussi la matrice composée des premiers membres de cette égalité est-elle le produit de la matrice (ω_i^{σ}) par sa transposée. D'où (2). Le lemme est démontré.

Pour tout isomorphisme $\varphi: L \to \mathbb{C}$ il existe son *conjugué* $\bar{\varphi}$: $x \mapsto \overline{x^{\varphi}}$, $x \in L$, où la barre surlignant x^{φ} symbolise le passage au conjugué complexe. Si $\varphi = \bar{\varphi}$, l'isomorphisme φ est dit *réel*, sinon il est appelé *complexe*.

Revenons au corps k. Soient $n = |k:\mathbb{Q}|$, s le nombre des isomorphismes réels $k \to \mathbb{C}$ et $2t$ le nombre des isomorphismes complexes, $n = s + 2t$. Soient $\sigma_1, \ldots, \sigma_s$ les isomorphismes réels et $\sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}$ les isomorphismes complexes.

Considérons l'espace euclidien $\mathbb{R}^n$ de dimension n et l'application $\sigma: k \to \mathbb{R}^n$ définie par la formule

$$x^{\sigma} = (x^{\sigma_1}, \ldots, x^{\sigma_s}, \mathrm{Re}\,(x^{\sigma_{s+1}}), \mathrm{Im}\,(x^{\sigma_{s+1}}), \ldots, \mathrm{Re}\,(x^{\sigma_{s+t}}), \mathrm{Im}\,(x^{\sigma_{s+t}})), \quad x \in k,$$

où Re, Im sont les parties réelle et imaginaire.

28.1.8. Exercice. L'application σ est un homomorphisme injectif du groupe additif de k dans le groupe additif de $\mathbb{R}^n$.

Soient maintenant k^*, k_0^* les groupes multiplicatifs du corps k et de l'anneau k_0 respectivement. Soit une application $\tau: k^* \to \mathbb{R}^{s+t}$ telle que

$$x^{\tau} = (\ln|x^{\sigma_1}|, \ldots, \ln|x^{\sigma_{s+t}}|), \quad x \in k^*.$$

28.1.9. Exercice. L'application τ est un homomorphisme du groupe k^* dans le groupe additif de $\mathbb{R}^{s+t}$.

28.1.10. Lemme. *L'ensemble k_0^{σ} est discret dans $\mathbb{R}^n$, i.e. son intersection avec une boule quelconque de $\mathbb{R}^n$ est au plus finie. L'ensemble $(k_0^*)^{\tau}$ est discret dans $\mathbb{R}^{s+t}$.*

Démonstration. Soit $\omega_1, \ldots, \omega_n$ une base du groupe additif de l'anneau k_0. Puisque $\det(\mathrm{tr}\,(\omega_i\omega_j)) \neq 0$ (lemme 28.1.5), les lignes

$$(\omega_i^{\sigma_1}, \ldots, \omega_i^{\sigma_s}, \omega_i^{\sigma_{s+1}}, \omega_i^{\bar{\sigma}_{s+1}}, \ldots, \omega_i^{\sigma_{s+t}}, \omega_i^{\bar{\sigma}_{s+t}}),$$
$$1 \leqslant i \leqslant n,$$

sont linéairement indépendantes sur $\mathbb{R}$ (lemme 28.1.7); par conséquent, les lignes $\omega_1^{\sigma}, \ldots, \omega_n^{\sigma}$ sont linéairement indépendantes sur $\mathbb{R}$,

i.e. forment une base de l'espace euclidien $\mathbb{R}^n$. Choisissons dans $\mathbb{R}^n$ une base biorthogonale $\{e_j\}$, i.e. telle que

$$(\omega_i^\sigma, e_j) = \delta_{ij},$$

où les parenthèses désignent le produit scalaire dans $\mathbb{R}^n$.

Soient

$$x \in k_0, \quad x = \sum x_i \omega_i, \quad x_i \in \mathbb{Z}.$$

Il est évident que $x^\sigma = \sum x_i \omega_i^\sigma$ et qu'en vertu de l'inégalité de Cauchy-Bouniakovski on a

$$| x_j | = | (x^\sigma, e_j) | \leqslant \| x^\sigma \| \cdot \| e_j \|.$$

Si x^σ appartient à une boule dans $\mathbb{R}^n$, on n'a pour les entiers x_j qu'un nombre fini de possibilités, d'où la première assertion du lemme. Dans le cas où $x \in k_0^*$ et x^τ appartient à une boule $\| z \| < r$ dans $\mathbb{R}^{s+t}$, alors x^σ appartient à une boule de rayon $e^r \sqrt{n}$ dans $\mathbb{R}^n$. Le lemme est démontré.

28.1.11. Exercice. Le noyau de la restriction de τ à k_0^* est l'ensemble de toutes les racines de 1 contenues dans k. Cet ensemble a une structure de groupe cyclique fini.

Indication: si $x^\tau = 0$, on a $\| x^\sigma \| \leqslant \sqrt{n}$.

28.1.12. Théorème. *Le groupe multiplicatif de l'anneau k_0 est de type fini.*

Démonstration. Conformément à l'exercice 28.1.11, il suffit de s'assurer que le groupe additif $A = (k_0^*)^\tau$ est de type fini, ce que nous ferons tout de suite. Soient $a_1, \ldots, a_m$ le sous-système maximal de A linéairement indépendant sur $\mathbb{R}$,

$$A' = \{\sum \alpha_i a_i \mid \alpha_i \in \mathbb{Z}\}, \quad A'' = \{\sum \alpha_i a_i \mid 0 \leqslant \alpha_i < 1\}.$$

Il est évident que tout $x \in A$ se laisse mettre sous la forme

$$x = x' + x'', \quad x' \in A', \quad x'' \in A''.$$

Puisque $x \in A$ et $x' \in A$, on a aussi $x'' \in A$. Or, l'ensemble A'' est borné dans $\mathbb{R}^{s+t}$, si bien que l'intersection $A \cap A''$ est finie (lemme 28.1.10). Par conséquent, l'indice $q = | A : A' |$ est fini. Puisque $qA \subset A'$, le groupe A est contenu dans un groupe additif engendré par $\frac{1}{q} a_1, \ldots, \frac{1}{q} a_m$. En vertu de l'exercice 8.1.7, le groupe A est de type fini. Le théorème est démontré.

Notons qu'il ressort de ce raisonnement que le nombre des générateurs libres de A est inférieur à $s + t$. Un raisonnement plus fin pourrait montrer que ce nombre est égal à $s + t - 1$ et que, par conséquent, k_0^* est le produit direct d'un groupe cyclique fini et de $s + t - 1$ groupes cycliques infinis (théorème de Dirichlet).

LITTÉRATURE

1. *Adjan S. I.* The Burnside problem and identities in groups. Berlin-Heidelberg-New York, Springer-Verlag, 1979 (traduit du russe).
2. *Aschbacher M.* The finite simple groups and their classification. Yale University Press, 1980.
3. *Bélonogov V. A., Fomine A. N.* Représentations matricielles en théorie des groupes finis. Moscou, « Naouka », 1976 (en russe).
4. *Birkhoff G.* Lattice theory. NY, 1948.
5. *Boussarkine V. M., Gortchakov Iou. M.* Groupes finis scindés. Moscou, « Naouka », 1968 (en russe).
6. *Chemetkov L. A.* Formations de groupes finis. Moscou, « Naouka », 1978 (en russe).
7. *Chunihin S. A.* Subgroups of finite groups. Groningen, Wolters-Noordhoff, 1969 (traduit du russe).
8. *Coxeter H. S. M., Moser W. O. J.* Generators and relations for discrete groups. Berlin-Heidelberg-New York, Springer-Verlag, 1972.
9. *Feit W., Thompson J. G.* Solvability of groups of odd order. Pacif. J. Math., 1963, 13, nº 3, p. 775-1029.
10. *Fuchs J.* Infinite abelian groups. Vol. 1. Pure and applied mathematics, Vol. 36. New York-London, Academic press, 1970.
11. *Gortchakov Iou. M.* Groupes aux classes finies d'éléments conjugués. Moscou, « Naouka », 1978 (en russe).
12. *Gruenberg K. W.* Cohomological topics in group theory. Lecture Notes in Mathematics, No. 143. Berlin-Heidelberg-New York, Springer-Verlag, 1970.
13. *Hall Jr. M.* The theory of groups. New York. Macmillan, 1959.
14. *Hall Ph.* The Edmonton notes on nilpotent groups. Queen Mary College mathematics notes. Mathematics Departmen, Queen Mary College, London, 1969.
15. *Huppert B.* Endliche Gruppen. I. Die Grundlehren der mathematischen Wissenschaften. Bd. 134. Berlin-Heidelberg-New York, Springer-Verlag, 1967; *Huppert B., Blackburn N.* Finite groups. II. III. Berlin, 1981.
16. *Kargapolov M. I.* Some questions in the theory of soluble groups. Lecture Notes in Mathematics. No. 372. Berlin-Heidelberg-New York, Springer-Verlag, 1974 (traduit du russe).
17. *Kegel O. H., Wehrfritz B. A. F.* Locally finite groups. North-Holland Mathematical Library. Amsterdam-London, North-Holland; New York, American Elsevier, 1973.
18. *Kokorin A. I., Kopytov V. M.* Fully ordered groups. New York, John Wiley and Sons, 1974 (traduit du russe).
19. *Kostrikin A. I.* Introduction à l'algèbre. Moscou, « Mir », 1981 (traduit du russe).

20. *Kurosh A. G.* The theory of groups. Vols. I, II. New York, Chelsea, 1960, (traduit du russe).
21. *Kurosh A. G., Chernikov S. N.* Soluble and nilpotent groups. American Math. Soc. Translation No. 80, 1953 (traduit du russe).
22. *Lyndon R. C., Schupp P. E.* Combinatorial group theory. Berlin-Heidelberg-New York, Springer-Verlag, 1977.
23. *Magnus W., Karrass A., Solitar D.* Combinatorial group theory: Presentations of groups in terms of generators and relations. Pure and Applied Mathematics, Vol. 13. New York, Interscience, 1966.
24. *Maltsev A. I.* Ecrits d'algèbre classique. Moscou, « Naouka », 1976 (en russe).
25. *Merzliakov Iou. I.* Groupes rationnels. Moscou, « Naouka », 1980 (en russe).
26. *Neumann H.* Varieties of groups. Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. 37. Berlin-Heidelberg-New York, Springer-Verlag, 1967.
27. *O'Meara O. T.* Lectures on linear groups. Published for the Conference Board of the Mathematical Sciences by the Amer. Math. Soc., Providence, 1974.
28. *Ovsiannikov L. V.* Groupes analytiques. Novossibirsk, 1972 (en russe).
29. *Pontrjagin L. S.* Topological groups. New York-London-Paris, Gordon and Breach, 1966 (traduit du russe).
30. *Puttaswamaiah B. M., Dixon J. D.* Modular representations of finite groups. New York, 1977.
31. *Robinson D. J. S.* A new treatment of soluble groups with finiteness conditions on their abelian subgroups. Bull. London Math. Soc., 1976, 8, No. 2, 113-129.
32. *Schmidt O. J.* Abstract theory of groups. San Fransisco-London, W. H. Freeman, 1966 (traduit du russe).
33. *Suprunenko D. A.* Matrix groups. Translations of math. monographs, Vol. 45. Providence, Amer. Math. Soc., 1976 (traduit du russe).
34. *Suzuki M.* Structure of a group and the structure of its lattice of subgroups. Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 10. Berlin-Göttingen-Heidelberg, Springer-Verlag, 1956.
35. *Tchernikov S. N.* Groupes dont le système de sous-groupes possède des propriétés données. Moscou, « Naouka », 1980 (en russe).
36. The Kourovka Notebook. Unsolved Problems in Group Theory. Transl. Amer. Math. Soc., v. 121, Providence, R. I., 1983 (traduit du russe).
37. Three lectures on polycyclic groups. London, Queen Mary College Math. Notes, 1973.
38. *Van der Waerden B. L.* Modern algebra. Vols. 1, 2. New York, Frederick Ungar, 1970.
39. *Vinogradov I. M.* Eléments de théorie des nombres. Moscou, « Naouka », 1981 (en russe).
40. *Wehrfritz B. A. F.* Infinite linear groups. Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. 76. New York-Heidelberg-Berlin, Springer-Verlag, 1973.
41. *Wielandt H.* Finite permutation groups. New York-London, Academic Press, 1964.
42. *Wussing H.* Die Genesis der abstrakten Gruppenbegriffes. Berlin, 1969.

INDEX ALPHABÉTIQUE

Action 88
Algèbre 13, 238
— associée 239
— enveloppante 239
— de Lie 239
— nilpotente 239
Anneau de groupe 98
Application polynomiale 143
Approximabilité 51
Associativité 14, 238
Automorphisme 52
— extérieur 53
— intérieur 53

Base 68
— d'un entrelacement 65
— de Maltsev 143
Bloc 99

Calcul des prédicats 248
Centralisateur 31
Centre 32
Classe d'éléments conjugués 29
— à gauche, à droite 26
— suivant un sous-groupe 26
Classes de conjugaison 29
Code génétique 112
Commutant 33
— réciproque 33
Commutateur 33, 239
— simple 121
Complété 80, 148
Composante 19
— primaire 82
Condition maximale 207
— minimale 207
— du normalisateur 154
Congruence 40
Conjugué d'un élément 28, 57
Connecteur 248
Coordonnées 143
Couche 58
Couronne de groupes 67

Déformation 231
— limite 233
Degré de liberté 68, 111, 124
— de nilpotence 129, 239
— de résolubilité 159
Demi-groupe 37
Dépendance linéaire 71
2-signalisateur 108
Dimension 71
— polycyclique 51

Elément générateur 21
— neutre 14
— non générateur 24
— périodique 134
— unité 14
Endomorphisme 52
Ensemble générateur 21
Entier algébrique 177, 253
Entrelacement 65, 99
— cartésien 65
Entrelacement direct 65
— standard 99

Exposant 16
Extension 48, 62
— scindée 62

Facteur 18
Filtre 248
Finitude résiduelle 52
Flexibilité 197, 199
Fonction de choix 118
— représentative 118
Fondation d'un entrelacement 65
Formule objet-universelle 249
— prénexe 249
— quasi universelle 249
— universelle 249
Fraction p-aire 17

Groupe 14
— abélien 16
— — élémentaire 59
— actif 65
— additif 16
— alterné 20, 105
— apériodique 15
— artinien 207
— sans centre 32
— de centre trivial 32
— commutatif 16
— complet 77
— complètement réductible 166
— cyclique 24
— dérivé 33
— diagonal 18
— divisible 77
— engélien 156
— à engendrement fini 21
— extrémal 208
— fini 16
— hyperrésoluble 160
— infini 16
— injectif 80
— libre 111
— — dans une classe 68
— linéaire général 17
— linéaire spécial 18
— — — projectif 105
— localement cyclique 25
— — fini 28, 191
— — $\mathfrak{m}$-engendré 25
— — nilpotent 151
— — normal 47
— matriciel général 17
— $\mathfrak{m}$-engendré 21
— mixte 15
— multiplicatif 17
— nilpotent 129
— nœthérien 207
— opérant sur un ensemble 88
— ordonnable 184, 249
— orthogonal 21
— parfait 59
— passif 65
— périodique 15, 191
— polycyclique 48
— préordonnable 249
— de présentation finie 112
— primaire 16

Groupe primitif 99
— projectif 80
— quasi cyclique 17
— quotient 39
— réductible 165-166
— résoluble 159
— r fois transitif 99
— de Schmidt 28
— simple 29, 57
— symétrique 17
— de Tchernikov 208
— sans torsion 15
— transitif 99
— trigonal 18
— trigonalisable 173
— de type fini 21
— unitaire 21
— unitrigonal 18
Groupes semblables 100

Hauteur d'un élément 83
Holomorphe 62
Homomorphisme 38
— canonique 40
— naturel 40
Hypercentre 129

Identité 123
Indice d'un sous-groupe dans le groupe 26
Induite, opération 19
Injection de Frobenius 66
Inverse, élément 14
Isomorphisme 14, 50, 100, 247

Localement 187
Logarithme 122

Matriochka 48
— centrale 128, 183
— normale 48
— plus fine 50, 182
— polycyclique 48
— résoluble 159, 183
— sous-normale 48, 182
— transfinie croissante 69
Méthode de recensement des classes suivant un sous-groupe 112
— de séparation des coordonnées 147
Mot 109
— réductible 109

N-groupe 183
$\tilde{N}$-groupe 183
Nil-algèbre 242
Nombre algébrique 177, 253
— p-adique 54
Normalisateur 29
Noyau de l'homomorphisme 39

Opérateurs 59
Opération algébrique 14, 247
Orbite 88, 199
Ordre 15-16

Partie périodique 81, 134
p-filet 62
p-groupe 16
Période 15-16
Poids du commutateur 121
Prédicat 247
Présentation du groupe 112
Presque 142
Produit cartésien de groupes 18
— complet 67
Produit direct 19, 45
— discret 67
— semi-direct 62
— sous-cartésien 47
— sous-direct 46
Projection 19
Puissance 15, 58

Quantificateur 248
Quotient 14

Rang 25
Recouvrement local 187, 247
Relateurs 112
Relations fondamentales 112
Représentant 26
Représentation 166
— monomiale 98
RI-groupe 183
$\overline{RI}$-groupe 183
RI^*-groupe 183
RN-groupe 183
$\overline{RN}$-groupe 183
RN^*-groupe 183

Section 48
Série centrale 129
— — inférieure 121, 129
— — supérieure 129
— de commutants 33
— dérivée 33
Signature 247
Sommant 19
Somme 19
— directe 45
Sous-groupe 19
— de Carter 164
— de congruence 43-44, 130
— distingué 28
— de Frattini 24
— de Hall 162
— invariant 28
— maximal 23
— normal 28
— permis 57
— propre 20
— pur 84
— sous-normal 48
— de Sylow 88
— verbal 123
— véritable 20
— vrai 20
Subdivision d'une matriochka 50, 182
Support 19
Système algébrique
— centré 248
— schreiérien 119

Tapis d'idéaux 130
Terme 19
— central 121, 129
Théorème local 187
Transformation élémentaire 23, 75-76
Transvection 22
Type de la suite 200

Ultrafiltre 248
Unité, élément 14

Variété 123

Z-groupe 183
$\tilde{Z}$-groupe 183
$\tilde{Z}A$-groupe 183
$\tilde{Z}D$-groupe 183

Préface à l'édition française 5
Notations canoniques 6
Introduction 8

Chapitre premier. DÉFINITION ET PARTIES PRINCIPALES D'UN GROUPE 13

§ 1. Définition d'un groupe 13
1.1. Axiomatique. Isomorphisme (13). 1.2. Exemples (15).
§ 2. Sous-groupes. Le sous-groupe normal 19
2.1. Sous-groupes (19). 2.2. Ensembles générateurs (21). 2.3. Groupes cycliques et localement cycliques. Rang (24). 2.4. Classes suivant un sous-groupe (26). 2.5. Classes d'éléments conjugués (28).
§ 3. Centre. Commutant 31
3.1. Centre (31). 3.2. Commutant (33).

Chapitre 2. HOMOMORPHISMES 38

§ 4. Homomorphismes et groupes quotients 38
4.1. Définitions (38). 4.2. Théorèmes des homomorphismes (41). 4.3. Produits sous-cartésiens (45). 4.4. Matriochkas (48).
§ 5. Endomorphismes. Automorphismes 52
5.1. Définitions (52). 5.2. Sous-groupes permis (57). 5.3. Groupes parfaits (59).
§ 6. Extensions par automorphismes 61
6.1. Holomorphe (61). 6.2. Entrelacements (64)

Chapitre 3. GROUPES ABÉLIENS 68

§ 7. Groupes abéliens libres. Dimension 68
7.1. Groupes abéliens libres (68). 7.2. Dimension d'un groupe abélien (71).
§ 8. Groupes abéliens de type fini 74
§ 9. Groupes abéliens complets 77
§ 10. Groupes abéliens périodiques 81

Chapitre 4. GROUPES FINIS 88

§ 11. Sous-groupes de Sylow 88
11.1. Théorème de Sylow (88). 11.2. Application aux groupes d'ordre pq (90). 11.3. Exemples de sous-groupes de Sylow (92.).
§ 12. Groupes de permutations 94
12.1. Représentation régulière (95). 12.2. Représentations par permutations des classes suivant un sous-groupe (97). 12.3. Transitivité. Primitivité (99).
§ 13. Groupes finis simples 102
13.1. Groupes alternés (103). 13.2. Groupes linéaires spéciaux projectifs (105).

Chapitre 5. GROUPES LIBRES ET VARIÉTÉS 109

§ 14. Groupes libres 109
14.1. Définition (109). 14.2. Représentation matricielle (115). 14.3. Sous-groupes (118). 14.4. Séries centrales et séries dérivées (121).
§ 15. Variétés 123
15.1. Identités et variétés (123). 15.2. Une autre approche des variétés (126).

Chapitre 6. GROUPES NILPOTENTS 128

§ 16. Propriétés générales et exemples 128
16.1. Définition (128). 16.2. Propriétés générales (132). 16.3. Groupes nilpotents d'automorphismes (136).
§ 17. Quelques sous-classes importantes 138
17.1. Groupes nilpotents finis (138). 17.2. Groupes nilpotents de type fini (141). 17.3. Groupes nilpotents sans torsion (148).
§ 18. Généralisations de la nilpotence 151
18.1. Nilpotence locale (151). 18.2. Condition du normalisateur (153). 18.3. Condition d'Engel (155).

Chapitre 7. GROUPES RÉSOLUBLES 158

§ 19. Propriétés générales et exemples 158
19.1. Définitions (158). 19.2. Groupes polycycliques et groupes hyperrésolubles (16).
§ 20. Groupes résolubles finis 162
20.1. Sous-groupes de Hall et de Carter (162). 20.2. Sur la réductibilité complète des représentations (165). 20.3. Critère d'hyperrésolubilité (170).
§ 21. Groupes de matrices résolubles 172
21.1. La presque trigonalisabilité (173). 21.2. Polycyclicité des groupes résolubles de $GL_n(\mathbb{Z})$ (177). 21.3. Les holomorphes des groupes polycycliques se plongent dans $GL_n(\mathbb{Z})$ (178).
§ 22. Généralisations de la résolubilité 182
22.1. Classes de Kouroch-Tchernikov (182). 22.2. Exemples (184). 22.3. Théorème local (187).

Chapitre 8. CONDITIONS DE FINITUDE 191

§ 23. La périodicité et la finitude locale 191
23.1. Ces deux notions coïncident-elles ? (191). 23.2. Le 2-groupe infini 2-engendré des transformations séquentielles (192). 23.3. Autre démonstration (202).
§ 24. Conditions minimale et maximale 207
24.1. Définitions et exemples (207). 24.2. Passage des sous-groupes abéliens au groupe résoluble (210). 24.3. Sur les groupes localement résolubles (215).
§ 25. La finitude du rang 221
25.1. Exemples (221). 25.2. Passage des sous-groupes abéliens au groupe résoluble (225). 25.3. Sur les groupes localement résolubles (230).

Appendice. QUELQUES RAPPELS D'ALGÈBRE, DE LOGIQUE ET DE THÉORIE DES NOMBRES 238

§ 26. Sur les algèbres nilpotentes 238
26.1. Nilpotence d'une algèbre associative et d'une algèbre de Lie (238). 26.2. Les nil-algèbres non nilpotentes (242).
§ 27. Théorèmes locaux de la logique 247
27.1. Systèmes algébriques (247). 27.2. Langage du calcul des prédicats (248). 27.3. Théorèmes locaux (250).
§ 28. Sur les entiers algébriques 253

Littérature 259
Index alphabétique 261

À NOS LECTEURS

Les Editions Mir vous seraient très reconnaissantes de bien vouloir leur communiquer votre opinion sur le contenu de ce livre, sa traduction et sa présentation, ainsi que toute autre suggestion.

Notre adresse : Editions Mir,
2, Pervi Rijski péréoulok, Moscou, I-110, GSP, U.R.S.S.

Imprimé en Union Soviétique